

Nos. 23-13698-E

---

---

**UNITED STATES COURT OF APPEALS  
FOR THE ELEVENTH CIRCUIT**

---

COIN CENTER, et al.,  
*Plaintiffs-Appellees,*

v.

SECRETARY, U.S. DEPARTMENT OF THE TREASURY, et al.,  
*Defendants-Appellants.*

---

Appeal from the U.S. District Court for the Northern District of Florida,  
No. 3:22-cv-20375-TKW-ZCB (Wetherell, J.)

---

**APPENDIX OF APPELLANTS COIN CENTER, ET AL.  
VOL. 3 of 3**

---

J. Abraham Sutherland  
106 Connally Street  
Black Mountain, NC 28711  
(805) 689-4577

Jeffrey M. Harris  
Cameron T. Norris  
Jeffrey S. Hetzel  
CONSOVOY MCCARTHY PLLC  
1600 Wilson Boulevard, Suite 700  
Arlington, Virginia 22209  
(703) 243-9423  
cam@consovoymccarthy.com

*Counsel for Coin Center et al.*

---

---

**CASE NO. 23-13698****INDEX TO DOCUMENT REFERENCES IN APPENDIX**

<b><u>Description of Item</u></b>	<b><u>Record Entry No.</u></b>	<b><u>Appendix Tab No.</u></b>
<b><u>VOLUME 1</u></b>		
<b>DISTRICT COURT DOCKET SHEET</b>		
Case No. 3:22-cv-20375-TKW-ZCB .....	N/A	DKT
<b>FIRST AMENDED COMPLAINT</b>		
(12/08/2022) .....	R.9	9
<b>ANSWER</b>		
(01/09/2023) .....	R.17	17
<b>PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT</b>		
(05/26/2023) .....	R.36	36
<b><u>Exhibit A</u></b>		
<b>DECLARATION OF PATRICK O'SULLIVAN.....</b>	R.36-2	
<b><u>Exhibit B</u></b>		
<b>DECLARATION OF JOHN DOE .....</b>	R.36-3	
<b><u>Exhibit C</u></b>		
<b>DECLARATION OF DAVID HOFFMAN .....</b>	R.36.4	
<b><u>Exhibit D</u></b>		
<b>DECLARATION OF JERRY BRITO, EXECUTIVE DIRECTOR OF COIN CENTER.....</b>	R.36-5	

<u>Description of Item</u>	<u>Record Entry No.</u>	<u>Appendix Tab No.</u>
<b>JOINT APPENDIX OF ADMINISTRATIVE RECORD DOCUMENTS CITED IN PARTIES' CROSS-MOTIONS FOR SUMMARY JUDGMENT (08/18/2023) .....</b>	<b>R.68</b>	<b>68</b>

**JOINT APPENDIX VOLUME I..... R.68-1**

**Designation and Blocking Memorandum  
A.R. 1-5**

**Press Release  
A.R. 9-12**

**Evidentiary Memorandum  
A.R. 13-100**

## **VOLUME 2**

**Exhibit 6: CoinDesk, *Tornado Cash Co-Founder Says the Mixer Protocol is Unstoppable*  
A.R. 137-149**

**Exhibit 7: Decrypt.co, *Tornado Cash Ethereum Token Down 50% After Sanctions*  
A.R. 150-157**

**Exhibit 15: Medium, *Tornado Cash Introduces Arbitrary Amounts & Shielded Transfers*  
A.R. 184-189**

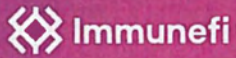
<b><u>Description of Item</u></b>	<b><u>Record Entry No.</u></b>	<b><u>Appendix Tab No.</u></b>
<b>Exhibit 54: Department of the Treasury, <i>Treasury Takes Robust Actions to Counter Ransomware</i> A.R. 474-479</b>		
<b>Exhibit 58: Ethereum, <i>Ethereum Accounts</i> A.R. 505-513</b>		
<b>Exhibit 59: Chainalysis, <i>Dissecting the DAO: Web3 Ownership is Surprisingly Complicated</i> A.R. 514-525</b>		
<b>Exhibit 62: Coin Center, <i>How Does Tornado Cash Work?</i> A.R. 544-576</b>		
<b>Exhibit 63: Chainalysis, <i>Crypto Mixers and AML Compliance</i> A.R. 577-582</b>		
<b>Exhibit 72: FIOD, <i>Arrest of Suspected Developer of Tornado Cash</i> A.R. 629-631</b>		
<b>Exhibit 86: GitHub, <i>Tornado Repositories/ Tornado Classic UI</i> A.R. 714-716</b>		
<b>Exhibit 89: Crypto.com, <i>Crypto Tokens vs. Coins – What’s the Difference?</i> A.R. 727-737</b>		
<b>Exhibit 103: Ethereum, <i>Intro to Ethereum</i> A.R. 814-821</b>		



<b><u>Description of Item</u></b>	<b><u>Record Entry No.</u></b>	<b><u>Appendix Tab No.</u></b>
<b>Exhibit 107: Ethereum, <i>Transactions</i> A.R. 856-872</b>		
<b>Exhibit 108: Certik, <i>What is Blockchain Analysis?</i> A.R. 873-883</b>		
<b>JOINT APPENDIX VOLUME II.....</b>	<b>R.68-2</b>	
<b>Exhibit 120: Tornado Cash, <i>Introduction</i> A.R. 950-954</b>		
<b>Exhibit 130: National Institute of Standards and Technology, <i>Blockchain Technology Overview</i> A.R. 1030-1152</b>		
<b>Exhibit 157: Ethereum, <i>Decentralized Autonomous Organizations</i> A.R. 1312-1322</b>		
<b><u>VOLUME 3</u></b>		
<b>Exhibit 175: Immunefi, <i>Tornado Cash Bug Bounties</i> A.R. 1577-1593</b>		
<b>Exhibit 176: Crypto News Australia, <i>Tornado Cash Token (TORN) Surges 94% Following Bullish Protocol Updates</i> A.R. 1594-1599</b>		
<b>Exhibit 179: Attorney General's Cyber Digital Task Force, <i>Cryptocurrency Enforcement Framework</i> A.R. 1752-1835</b>		

<u>Description of Item</u>	<u>Record Entry No.</u>	<u>Appendix Tab No.</u>
<b>Exhibit 184: BeinCrypto, <i>Ethereum Name Service (ENS): Everything You Need to Know</i></b> <b>A.R. 1931-1944</b>		
<b>Exhibit 199: Harvard Law School Forum on Corporate Governance, <i>An Introduction to Smart Contracts and Their Potential and Inherent Limitations</i></b> <b>A.R. 2140-2149</b>		
<b>ORDER ON CROSS-MOTIONS FOR SUMMARY JUDGMENT</b> <b>(10/30/2023) .....</b>	<b>R.74</b>	<b>74</b>
<b>JUDGMENT</b> <b>(10/30/2023) .....</b>	<b>R.75</b>	<b>75</b>

# EXHIBIT 175



## Tornado Cash

[Submit a Bug](#)

Live since

KYC required

Maximum bounty

Rewards by Trust Level



## Program Overview

Tornado Cash is a fully decentralized non-custodial protocol allowing private transactions in the crypto-space. Tornado Cash improves transaction privacy by breaking the on-chain link between source and destination addresses. It uses a smart contract that accepts ETH & other token deposits from one address and enables their withdrawal from a different address.

As a non-custodial protocol, users keep custody of their cryptocurrencies while operating Tornado Cash. At each deposit, users are provided with the private key enabling the access to the deposited funds, which gives users complete control over their assets.

For more information about Tornado Cash, please visit

<https://tornado.cash/>.

This bug bounty program is focused on their smart contracts and is focused on preventing:

- Thefts or freezing of funds in anonymity pool
- Thefts or freezing of unclaimed yield (TORN anonymity mining)
- Theft of governance funds (Main on-chain Tornado DAO treasury only)
- On chain governance activity disruption

## Rewards by Threat Level

Rewards are distributed according to the impact of the vulnerability based on the **Immunefi Vulnerability Severity Classification System**. This is a simplified 5-level scale, with separate scales for websites/apps and smart contracts/blockchains, encompassing everything from consequence of exploitation to privilege required to likelihood of a successful exploit.

All smart contract bug reports must come with a PoC in order to be considered for a reward.

This bug bounty program has fixed rewards in **TORN**. The USD amounts reflected are only estimates. For an up-to-date price of the token, please visit <https://tornado.cash/>.

Critical smart contract vulnerabilities are further capped at 10% of economic damage, primarily taking into account the funds at risk. However, there is a minimum reward of **2 000 TORN**. Additionally, the maximum reward is capped at 32 500 TORN, even if 10% of the damage in USD equivalent is greater than the USD equivalent of 32 500 TORN.

Payouts are handled by the **Tornado Cash** team directly and are denominated in TORN. Payouts are done in **TORN**.

## Smart Contract

**Critical**

Level

**Up to 32,500 TORN (-Up to USD \$1,300,000)**

Payout

**PoC Required**

**High**

Level

**1,625 TORN (~USD \$65,000)**

Payout

**PoC Required**

**Medium**

Level

**525 TORN (~USD \$21,000)**

Payout

**PoC Required**



## Assets in scope

<https://web.archive.org/web/20220527111152/https://ether...>

Target

Smart Contract - 0.1 ETH Pool

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

Smart Contract - 1 ETH Pool

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

Smart Contract - 10 ETH Pool

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target



**Smart Contract - 100 ETH Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 100 DAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 1k DAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 10k DAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 100k DAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 5k cDAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 50k cDAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 500k cDAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 5m cDAI Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 100 USDC Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 1k USDC Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 100 USDT Pool**

Type



<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 1k USDT Pool**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 0.1 WBTC**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 1 WBTC**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - 10 WBTC**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - Torn Token**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - Governance Proxy**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - Reward Verifier**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - Withdraw Verifier**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - Tree Update Verifier**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - Reward Swap**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - TornadoCash Proxy**

Type



<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - TornadoTrees**

Type

<https://web.archive.org/web/20220527111152/https://ether...>

Target

**Smart Contract - Miner**

Type

<https://web.archive.org/web/20220527111152/https://githu...>

Target

**Smart Contract - Poseidon hasher**

Type

All smart contracts of Tornado Cash can be found at

<https://github.com/tornadocash>. However, only those in the Assets in Scope table are considered as in-scope of the bug bounty program.

## Impacts in scope

Only the following impacts are accepted within this bug bounty program.  
All other impacts are not considered as in-scope, even if they affect something in the assets in scope table.

### Smart Contract

**Theft of governance funds (Main on-chain Tornado DAO treasury only)**

**Critical**

Impact

**Thefts or freezing of unclaimed yield (TORN anonymity mining)**

**High**

Impact

## Out of Scope & Rules

The following vulnerabilities are excluded from the rewards for this bug bounty program:

- Attacks that the reporter has already exploited themselves, leading to damage
- Attacks requiring access to leaked keys/credentials



- Attacks requiring access to privileged addresses (governance, strategist)

## Smart Contracts and Blockchain

- Incorrect data supplied by third party oracles
  - Not to exclude oracle manipulation/flash loan attacks
- Basic economic governance attacks (e.g. 51% attack)
- Severe break of privacy due to issues with the SNARK logic/code
- Lack of liquidity
- Best practice critiques
- Sybil attacks
- Centralization risks

The following activities are prohibited by this bug bounty program:

- Any testing with mainnet or public testnet contracts; all testing should be done on private testnets
- Any testing with pricing oracles or third party smart contracts
- Attempting phishing or other social engineering attacks against our employees and/or customers
- Any testing with third party systems and applications (e.g. browser extensions) as well as websites (e.g. SSO providers, advertising networks)
- Any denial of service attacks
- Automated testing of services that generates significant amounts of traffic

- Public disclosure of an unpatched vulnerability in an embargoed bounty

**Explore**

**Hackers**

**Projects**

**Priority One**

**Nexus Matching**

**Whitehat Scholarship**

**About**

**Rules**

**Press**

**Brand Assets**

**Crypto Losses Report**



[Blog](#)

[Contact](#)

[Privacy](#)

[Careers](#)

Hackers subscribed to our newsletter are 35.8% more likely to earn a Bounty

Your email, please

Prove it

[Twitter](#)

[Discord](#)

[Medium](#)

[Youtube](#)

[LinkedIn](#)

Copyright © Immunefi – Crypto bug bounty platform

# EXHIBIT 176





**Bitcoin**  
\$30,383 AUD  
▼ -0.43%

**Ethereum**  
\$2,081 AUD  
▼ -0.21%

**Tether**  
\$1.56 AUD  
▼ -0%

**USD Coin**  
\$1.57 AUD  
▼ -0%

**BNB**  
\$446 AUD  
▼ -0.05%

live prices by [Swift.com.au](https://www.swift.com.au)

# Tornado Cash Token (TORN) Surges 94% Following Bullish Protocol Updates



Monday, September 26, 2022, 9:31 AM  
**Jody McDonald**  
Crypto News Writer

The native token for the Tornado Cash protocol (TORN), an Ethereum-based privacy protocol, has surged 94 percent following the launch of its latest network updates.

Tornado Cash is a fully decentralised privacy protocol which enables anonymous transactions on the Ethereum network. The protocol achieves anonymity primarily by breaking the on-chain link between source and destination addresses when transactions are made.

I have seen a bit of [@TornadoCash](#) hate recently. This is ridiculous. There are many reasons other than crime that a person would want privacy. Here is a short list.

— Oxacti (@Oxacti) [February 14, 2022](#)

Top ↑



## Price Increase Follows Launch Of Relayers

The latest price action for TORN follows the adoption and implementation of the protocol's 10th on-chain governance proposal, which saw the addition of relayers to the network:

@TornadoCash relayer registry proposal #10 is definitely bullish for \$TORN holders 🚀✅  
With the latest governance proposal about to be validated, I'm making a point about why this is so beneficial to \$TORN valuation.



— bt11ba (@bt11ba) February 16, 2022

The community voted overwhelmingly in favour of the proposal, which was accepted on February 19. Following the launch of relayers on March 2, the price of TORN spiked from around US\$37 to around the \$US67 mark.

## What Are Relayers?

Tornado Cash relayers are community members who process withdrawal transactions and allow users to send transactions to accounts with no ETH balance – they are considered an important part of the protocol and improve users' privacy.

Relayers are compensated for their network services with a small portion of users' deposits. Anyone can become a relayer, provided they meet the minimum balance requirement of 300 TORN and accept the terms and conditions.

## TORN Gaining Momentum

The addition of relayers to the Tornado Cash protocol is a further boost following its integration of ETH layer 2 solution Arbitrum in December 2021, which saw a dramatic decrease in gas fees and improvements in transaction times:

4/4 📄 Final Score: 85% 🔥 #DeFi #ETH #MATIC #AVAX #BSC  
\$TORN[@semenov\\_roman](https://t.co/4Fs1fQ8uRK) @TornadoCash @bt11ba  
@WUTornado @rstormsf @WillMcTighe @kaili\_jenner @mike\_h\_wu  
— DeFiSafety (@DefiSafety) March 1, 2022

The protocol was also recently assessed by DeFi safety, which found it to be highly secure – awarding Tornado Cash an overall score of 85 percent.

Top ↑



## Share this article



Join in the conversation on this article's [Twitter thread](#).

*Disclaimer: The content and views expressed in the articles are those of the original authors own and are not necessarily the views of Crypto News. We do actively check all our content for accuracy to help protect our readers. This article content and links to external third-parties is included for information and entertainment purposes. It is not financial advice. Please do your own research before participating.*

## Related News



### DEFI

[DeFi needs appropriate regulation before moving to retail, says Fed Chair: Finance Redefined](#)

4 hours ago by Cointelegraph



### NFTS

[Starfish Finance Proposes DeFi-NFT Convergence on Polkadot](#)

4 hours ago by Usethebitcoin

## Trusted Partners



Crypto Trading Education

[View all partners](#)

## Trending

### RIPPLE

[Popular Crypto Analyst Doubles Down on Explosive \\$XRP Price Prediction](#)

#1

### BITCOIN

[Markets: XRP jumps amid court ruling against SEC, Bitcoin gains, Ether sole loser in crypto top 10](#)

#2

### TERRA







[Crypto Trader Says One Altcoin That's Exploded 120% This Month Is About To Nuke – Here's His Target](#)

#3

## Popular

Top ↑

**REVIEW**[The Best Crypto Exchanges for Australia](#)**EVENT**[Australia Crypto Convention - Gold Coast, Sep 2022](#)**Today's Top Gainers**

	<a href="#">SAFEMOON</a>	<b>\$8.39</b>	<b>▲ 57.72%</b>
	<a href="#">LUNC</a>	<b>\$0.00</b>	<b>▲ 6.09%</b>
	<a href="#">QNT</a>	<b>\$224.0</b>	<b>▲ 5.91%</b>
	<a href="#">FX</a>	<b>\$0.38</b>	<b>▲ 5.24%</b>
	<a href="#">HNT</a>	<b>\$8.39</b>	<b>▲ 5.12%</b>
	<a href="#">TON</a>	<b>\$2.10</b>	<b>▲ 4.72%</b>

[View more](#) powered by [Swyftx.com.au](#)

**Top Daily News**
 Your email address

Go

**Real-Time News**Follow  
on TwitterJoin  
on TelegramSubscribe  
on Google News**AUSTRALIA**

Crypto News provides you with the most relevant Bitcoin, cryptocurrency & blockchain news.

**Useful links**

[News Archive](#)  
[Sponsored Articles](#)  
[Institution Crypto Purchases](#)  
[Crypto Whale Transactions](#)

**About Us**

[About](#)  
[Writers](#)  
[Partners](#)  
[Affiliates](#)  
[Advertise](#)  
[Contact](#)

Are you a journalist or an editor? Join us: [editor@cryptonews.com.au](mailto:editor@cryptonews.com.au)

Top ↑



9/30/22, 9:31 PM

Tornado Cash token (TORN) Surges 94% Following Bullish Protocol Updates

By using this website, you agree to our Terms of Use and Privacy Policy. Crypto News Australia is a news website that is dedicated to providing the highest journalistic standards and adheres to its Editorial Policy. Crypto News Australia are a subsidiary of Swyftx Pty Ltd, which operates a cryptocurrency exchange in Australia and New Zealand. Any affiliations or relationships are outlined in our Partners page or Affiliates page. Our website is purely informational and provides news about cryptocurrency & blockchain. The information on Crypto News Australia should not be taken as financial advice, investment advice or a personal recommendation. Buying and trading cryptocurrencies is a high-risk activity. Please do your own due diligence before making any investment decisions. We are not accountable, directly or indirectly, for any damage or loss incurred, alleged or otherwise, in connection to the use or reliance of any content you read on this or any affiliated website.

© Crypto News Pty Ltd 2017 - 2022 ABN 88 611 395 067

[Terms](#) [Privacy policy](#) [Refund policy](#) [Cookies policy](#) [Editorial policy](#)  
[Trademarks](#)

Top ↑

# EXHIBIT 179



U.S. Department of Justice



REPORT OF THE  
ATTORNEY  
GENERAL'S  
**CYBER  
DIGITAL**  
TASK FORCE

**CRYPTOCURRENCY**

**ENFORCEMENT  
FRAMEWORK**

# REPORT OF THE ATTORNEY GENERAL'S **CYBER DIGITAL TASK FORCE**

Executive Summary: This report provides a comprehensive overview of the findings and recommendations of the Attorney General's Cyber Digital Task Force. The task force was established to address the challenges posed by cyber threats and digital privacy concerns. The report details the scope of the investigation, the methodology used, and the key findings. It also outlines the recommendations for improving cybersecurity and digital privacy protections. The report is intended for the Attorney General and other relevant stakeholders.



United States Department of Justice  
Office of the Deputy Attorney General  
Cyber-Digital Task Force  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530  
<https://www.justice.gov/cryptoreport>

*October 2020*

\*

\*

\*

**Guidance Disclaimer:** This document does not contain any new binding legal requirements not otherwise already imposed by statute or regulation. To the extent this Enforcement Framework is viewed as a guidance document within the definition of Executive Order 13891, the contents of this document do not have the force and effect of law and are not meant to bind the public in any way. If viewed as a guidance document, this document is intended only to provide clarity to the public regarding existing requirements under the law or Department of Justice policies.

---

## TABLE OF CONTENTS

ATTORNEY GENERAL’S CYBER-DIGITAL TASK FORCE .....	v
INTRODUCTION.....	vii
CRYPTOCURRENCY: AN ENFORCEMENT FRAMEWORK.....	1
PART I	
THREAT OVERVIEW.....	2
THE BASICS.....	2
LEGITIMATE USES .....	5
ILLICIT USES.....	5
THE ROLE OF DARKNET MARKETS.....	16
PART II	
LAW AND REGULATIONS .....	20
CRIMINAL CODE AUTHORITIES .....	20
REGULATORY AUTHORITIES.....	22
INTERNATIONAL REGULATION .....	35
PART III	
ONGOING CHALLENGES AND FUTURE STRATEGIES.....	37
BUSINESS MODELS AND ACTIVITIES THAT MAY FACILITATE CRIMINAL ACTIVITY.....	37
DEPARTMENT OF JUSTICE RESPONSE STRATEGIES .....	44
CONCLUSION.....	51





## ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE

### TASK FORCE MEMBERS

#### **Sujit Raman, Chair**

Associate Deputy Attorney General  
*Office of the Deputy Attorney General*

#### **John Brown**

Executive Assistant Director  
*Federal Bureau of Investigation*

#### **Brian C. Rabbitt**

Assistant Attorney General (Acting)  
*Criminal Division*

#### **John C. Demers**

Assistant Attorney General  
*National Security Division*

#### **Terry Wade**

Executive Assistant Director  
*Federal Bureau of Investigation*

#### **Andrew E. Lelling**

United States Attorney  
*District of Massachusetts*

#### **Beth A. Williams**

Assistant Attorney General  
*Office of Legal Policy*

---

### TASK FORCE CONTRIBUTORS

#### **Anthony M. Shults**

Senior Counsel, Office of Legal Policy  
*Staff Director*

Sabrina Bagdasarian  
Jeff Breinholt  
Thomas Burrows  
Richard W. Downing

Lindsey Freeman  
Christopher Hardee  
Adam Hickey  
Michele R. Korver  
Erin Mikita

Sean Newell  
C. Alden Pelker  
Kimberley Raleigh  
Leo Tsao

*And the Men and Women of the Federal Bureau of Investigation*







---

## INTRODUCTION

**I**nnovation can drive a society forward. But innovation does not occur in a vacuum. Public policy can establish background conditions that help the innovative spirit thrive—or create an environment in which that spirit is inhibited, or suppressed.

Even in societies where transformative scientific and technological advancements are achievable, public policy again plays a critical mediating role. In the wrong hands, or without appropriate safeguards and oversight, these advancements can facilitate great human suffering. Just ask the political enemies of authoritarian regimes that deploy surveillance tools Orwell never could have imagined. Or, closer to home, listen to the child victims of unspeakable sexual exploitation whose images and livestreamed abuse are so easily transmitted across the internet.

Technological innovation and human flourishing are complementary concepts, but the former does not guarantee the latter. Good public policy—and the fair and equitable enforcement of such policy—can help bring the two into alignment. And even as too much regulation undoubtedly stifles innovation (and human flourishing, too), the absence of law’s protections can endanger progress across both dimensions. It takes careful consideration, and a deep and ongoing immersion in the facts, to understand when, and how, law should intervene. Once law’s empire has established its root in a particular domain, it requires equally careful consideration (and humility on the part of government officials) to

ensure that regulation goes no further than is required—that government action, in other words, reflects enforcement only of “those wise restraints that make us free.”<sup>i</sup>

### **This Enforcement Framework**

In 2018, Attorney General Jeff Sessions established a Cyber-Digital Task Force within the U.S. Department of Justice to evaluate the impact that recent advances in technology have had on law enforcement’s ability to keep our citizens safe. Acknowledging the many ways in which technological advances “have enriched our lives and have driven our economy,” the Attorney General also noted that “the malign use of . . . technolog[y] harms our government, victimizes consumers and businesses, and endangers public safety and national security.”<sup>ii</sup>

The Task Force issued a comprehensive report later that year. That report identified particular threats currently confronting our society, ranging from transnational criminal enterprises’ sophisticated cyber-enabled schemes, to malign foreign influence operations, to efforts to compromise our nation’s critical infrastructure. The report also identified a number of emerging threats whose contours are still developing, and recommended further examination of their potential impact. Specifically, the report recommended that “the Department should continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use.”<sup>iii</sup> This Cryptocurrency Enforcement Framework represents the fruits of the Task Force’s efforts.



At the outset, it bears emphasizing that distributed ledger technology, upon which all cryptocurrencies build, raises breathtaking possibilities for human flourishing. These possibilities are rightly being explored around the globe, from within academia and industry, and from within governments—including our own.

It should be no surprise, for example, that researchers within the U.S. National Institute of Standards and Technology “have been investigating blockchain technologies at multiple levels: from use cases, applications and existing services, to protocols, security guarantees, and cryptographic mechanisms.”<sup>iv</sup> Or that the U.S. Department of Defense’s recently-issued Digital Modernization Strategy specifically identifies blockchain technology as having “promise to provide increased effectiveness, efficiency, and security.”<sup>v</sup> Or that the U.S. Food and Drug Administration recently released a detailed vision for how it plans to deploy blockchain for food safety-related purposes.<sup>vi</sup> Or that—in the cryptocurrency space specifically—“the Federal Reserve is active in conducting research and experimentation related to distributed ledger technologies and the potential use cases for digital currencies,” including by partnering with the Massachusetts Institute of Technology to “build and test a hypothetical digital currency oriented to central bank uses.”<sup>vii</sup> Without doubt, cryptocurrency represents a transformative way to store and exchange value.

But as the following pages make clear, despite its relatively brief existence, this technology already plays a role in many of the most significant criminal and national security

threats our nation faces. As the Task Force has found, illicit uses of cryptocurrency typically fall into three categories: (1) financial transactions associated with the commission of crimes; (2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; or (3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself. Part I of this Enforcement Framework examines in detail each of those categories.

Our society is not powerless in the face of these threats. As Part II demonstrates, the government has legal and regulatory tools available at its disposal to confront the threats posed by cryptocurrency’s illicit uses. Interagency partnership is critical for effectively leveraging those tools. The Department of Justice has built strong working relationships with its regulatory and enforcement partners in the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the U.S. Department of the Treasury (including FinCEN, OFAC, and the IRS), among others, to enforce federal law in both its civil and criminal aspects. We have actively participated in international regulatory and criminal enforcement efforts, as well.

Those efforts are paying off. The past year alone has witnessed the indictment and arrest of the alleged operator of the world’s largest online child sexual exploitation market, involving an enforcement action that was coordinated with the disruption of that darknet market, the rescue of over 20 child victims, and the seizure of hundreds of thousands of dollars’ worth of bitcoin; the largest-ever seizure of cryptocurrency in the terrorism context, stemming from the



dismantling of terrorist financing campaigns running into the millions of dollars involving Hamas's military wing, al-Qaeda, and ISIS; the first-ever imposition of economic sanctions for virtual-asset-related malicious cyber activity; and a novel (and successful) use of the federal securities laws to protect investors in the cryptocurrency space, resulting in the disgorgement of over \$1.2 billion in ill-gotten gains in a single case. We expect these enforcement trends to continue.

This report concludes in Part III with a discussion of the ongoing challenges the government faces in cryptocurrency enforcement—particularly with respect to business models (employed by certain cryptocurrency exchanges, platforms, kiosks, and casinos), and to activity (like “mixing” and “tumbling,” “chain hopping,” and certain instances of jurisdictional arbitrage) that may facilitate criminal activity.

### **The Challenges We Face**

Those challenges map neatly onto the broader set of challenges that many emerging technologies present to law enforcement. Blockchain-related technologies are complex and are difficult to learn; for example, the methods for executing crimes like pump-and-dump schemes are changing, and require investigators to familiarize themselves with everything from how initial coin offerings (ICOs) are conducted to how technologically-savvy people communicate on specialized communications applications. Not only are these emerging technologies difficult to learn, but the relevant markets also rapidly evolve. The ICO boom from a few years ago has given way to the exponential growth of Decentralized Finance markets in recent

months—with all the associated complexities and difficulties for enforcers seeking to stay ahead of the curve and keep investors safe.

The global nature of the blockchain ecosystem adds a further layer of complexity. Crime has been expanding beyond national borders for years, but blockchain takes this globalization to another level. Parties conduct transactions and transfers between continents in a matter of minutes, and the digital infrastructure of the blockchain itself almost always transcends territorial boundaries. Adding to the difficulty, some of the largest cryptoasset exchanges operate outside of the United States, and many still require nothing more than an unverified email address before allowing an individual to begin trading. Finally, decentralized platforms, peer-to-peer exchangers, and anonymity-enhanced cryptocurrencies that use non-public or private blockchains all can further obscure financial transactions from legitimate scrutiny. As this Enforcement Framework makes clear, the challenges are significant. But so, too, are the resources that the U.S. Department of Justice, as well as the U.S. government as a whole, are dedicating to the effort, in collaboration with our international partners.

### **The Web 3.0**

Technologists often talk about the Web 3.0, the next phase of the internet's evolution. On this vision, humans will reclaim the internet, their data, and their anonymity from large outside forces, whether they be corporate firms or government entities. Cryptocurrency—a medium of exchange defined, at its core, by a sense of private, individual control, and whose underlying



blockchain technology already provides the backbone for applications outside the digital currency context—is central to this decentralized, anonymized, and still-being-defined notion of a future in which “a more semantically intelligent web” leverages data that “will be used by algorithms to improve user experience and make the web more personalized and familiar,” and in which users will no longer have to “rely on network and cellular providers that surveil the information going through their systems.”<sup>viii</sup> Ultimately, the Web 3.0 is a vision about the nature of data itself, foretelling a world in which information is diffuse and dynamic—present everywhere at once, and therefore beyond any outsider’s grasp.

Only time will tell how, and in what form, the Web 3.0 finally takes shape. To its proponents, this vision marries technological innovation

with human flourishing. This Enforcement Framework suggests that, however liberating the emerging glimpses of the Web 3.0 might seem to be, that vision also can pose uniquely dangerous threats to public safety. Confronting and addressing those threats is what good public policy should do—and what the crypto ecosystem itself may have to do, if its vision of the future is ever fully to take hold. Meanwhile, federal authorities will continue vigorously enforcing the law as it exists, and pursuing justice on behalf of the American people.



– Sujit Raman, Chair,  
Attorney General’s Cyber-Digital Task Force



Deputy Attorney General Jeffrey A. Rosen announces on September 22, 2020 the results of Operation Disruptor, the U.S. government’s largest operation to date targeting criminal activity on the darknet. The operation resulted in the arrest of nearly 180 dark web drug traffickers and criminals; the seizure of approximately 500 kilograms of illegal drugs worldwide; and the seizure of millions of dollars in cash and virtual currencies.





---

## CRYPTOCURRENCY: AN ENFORCEMENT FRAMEWORK

Innovations in technology often change the world for the better. And yet, criminals, terrorists, and rogue states can use those same innovations for their own illegitimate ends, imposing great costs on the public. Today, few technologies are more potentially transformative and disruptive—and more potentially susceptible to abuse—than cryptocurrency.

Cryptocurrency is a form of virtual asset that uses cryptography to secure financial transactions. Many of cryptocurrency's central features—including decentralized operation and control, and, in some cases, a high degree of anonymity—present new and unique challenges for public safety that must be addressed, lest the technology be used predominantly for criminal activity. Indeed, despite its relatively brief existence, cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces. For example, cryptocurrency is increasingly used to buy and sell lethal drugs on the dark web (and by drug cartels seeking to launder their profits), contributing to a drug epidemic that killed over 67,000 Americans by overdose in 2018 alone.<sup>1</sup> Rogue states like Russia, Iran, and North Korea may turn to cryptocurrency to fund cyber-attacks, blunt the impact of U.S. and international sanctions, and decrease America's influence in the global marketplace. And, while terrorist use of cryptocurrency is still evolving, certain terrorist groups have solicited cryptocurrency donations running into the millions of dollars via online social media campaigns.

The U.S. Department of Justice is responsible for investigating and prosecuting crimes and threats to national security, including those facilitated by the use of cryptocurrency. As consumers, investors, financial institutions, elected officials, and other stakeholders consider the future path of cryptocurrency and related technologies, we are publishing this Framework to enhance understanding of the associated public safety and national security challenges that these technologies present. These challenges impact the security and legitimacy of the cryptocurrency ecosystem itself; only by identifying and responsibly addressing them can the risks of cryptocurrency be mitigated. At a minimum, this means that entities that use or are impacted by cryptocurrency must understand their legal obligations and invest in meeting them. For example, cryptocurrency exchanges—including those physically located outside the United States—must take seriously their legal and regulatory obligations, discussed in greater detail below, to protect users and to safeguard potential evidence in criminal or national security investigations. Where a breach of these obligations might rise to the level of a criminal violation, the Department will take appropriate action.



In the pages that follow, we:

(1) describe how cryptocurrency technology is currently used and illustrate how malicious actors have misused that technology to harm cryptocurrency users, exchanges, and investors, as well as to facilitate a broad range of crimes from child exploitation to terrorism;

(2) identify some of the key legal authorities and partnerships the Department has relied upon to combat criminal and national security threats involving cryptocurrency; and

(3) discuss approaches for addressing the growing public safety challenges related to cryptocurrency.

## I. Threat Overview

### A. The Basics

“Virtual currency” is a digital representation of value that, like traditional coin and paper currency, functions as a medium of exchange—i.e., it can be digitally traded or transferred, and can be used for payment or investment purposes. Virtual currency is a type of “virtual asset” that is separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets.<sup>2</sup> Moreover, unlike “traditional currency”—which is also referred to as fiat currency, real currency, or national currency—virtual currency does not have legal tender status in any particular country or for any government or other

**Figure 1: Systemic Attributes of Virtual Currency**





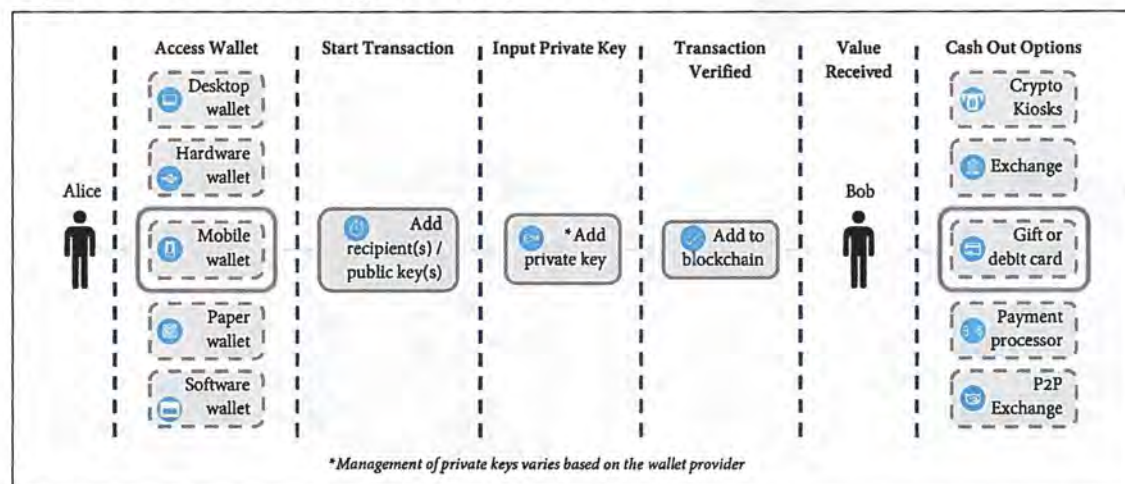
creditor.<sup>3</sup> Instead, the exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Virtual currency can be *convertible*, meaning it has an equivalent value in real currency or acts as a substitute for real currency, or *non-convertible*, meaning it is specific to a particular virtual domain—such as an online gaming community—and cannot be exchanged for real currency.<sup>4</sup>

“Cryptocurrency” refers to a specific type of virtual currency with key characteristics. The vast majority of cryptocurrencies are decentralized, as they lack a central administrator to issue currency and maintain payment ledgers—in other words, there is no central bank. Instead, cryptocurrencies rely on complex algorithms, a distributed ledger that is often referred to as the “blockchain,” and a network of peer-to-peer users to maintain an accurate system of payments and receipts. As their name suggests, cryptocurrencies rely on cryptography for

security. Some examples of cryptocurrencies include Bitcoin,<sup>5</sup> Litecoin, and Ether.

Cryptocurrency can be exchanged directly person to person; through a cryptocurrency exchange; or through other intermediaries. The storage of cryptocurrency is typically associated with an individual “wallet,” which is similar to a virtual account. Wallets can interface with blockchains and generate and/or store the public keys (which are roughly akin to a bank account number) and private keys (which function like a PIN or password) that are used to send and receive cryptocurrency. Cryptocurrency wallets can be housed in a variety of forms, including on a tangible, external device (“hardware wallets”); downloaded as software (“software wallets”) onto either a personal computer or server (“desktop wallets”) or an application on a smartphone (“mobile wallets”); as printed public and private keys (“paper wallets”); and as an online account associated with a cryptocurrency exchange.

Figure 2: Anatomy of a Cryptocurrency Transaction



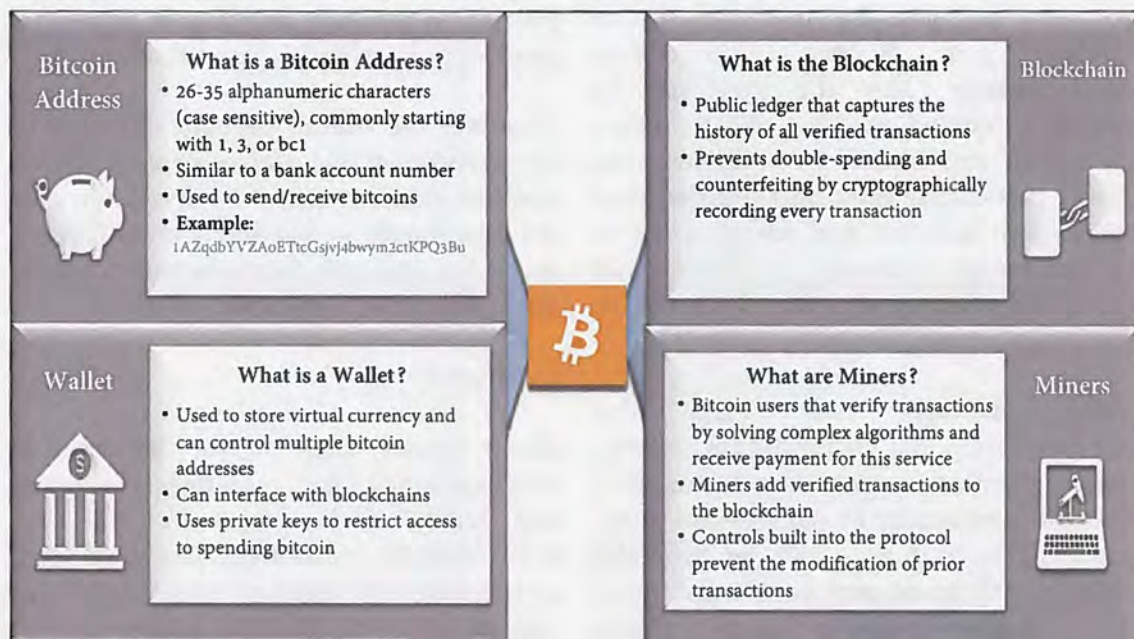


The distributed ledger—which, as noted above, is known as the “blockchain” for most cryptocurrencies—allows such a decentralized system to accurately track payments and to prevent double-spending and counterfeiting by cryptographically recording every transaction. When a transaction is initiated, it is shared with participants on the network associated with

payment in the cryptocurrency itself—a process known as “mining.”

Cryptocurrencies can vary in their degree of anonymity depending on the public or non-public nature of their associated blockchain. For instance, while Bitcoin addresses do not have names or specific customer information attached to them, Bitcoin’s blockchain is

**Figure 3: Bitcoin Basics – Key Terms**



the particular cryptocurrency, whereupon special users (often called “miners”) verify that the units have not already been spent, and validate the transaction by solving a complex algorithm. The transaction is then added to the blockchain, with each block consisting of a group of reported transactions in chronological order. In exchange for participating in this community validation process, miners generate and receive a

public. As a result, users can query addresses to view and understand Bitcoin transactions to some extent. Other cryptocurrencies, however, use non-public or private blockchains that make it more difficult to trace or to attribute transactions. These are often referred to as “anonymity enhanced cryptocurrencies” (“AECs”) or “privacy coins.” Examples of AECs include Monero, Zcash, and Dash.



---

## **B. Legitimate Uses**

Cryptocurrency advocates maintain that a decentralized, distributed, and secure cryptocurrency holds great promise for legitimate use. Today's market includes over 2,000 cryptocurrencies, which enable users to transfer virtual currency around the globe in exchange for goods, services, and other sources of value. Proponents of cryptocurrency contend that, by eliminating the need for financial intermediaries to validate and facilitate transactions, cryptocurrency has the potential to minimize transaction costs and to reduce corruption and fraud. In addition, some users—particularly those in countries beset by rampant inflation and where access to normal foreign exchange is limited—may use virtual currency to avoid inflation in fiat currencies.

Some advocates also claim that cryptocurrency may in the future facilitate “micro-payments,” providing enterprises with the opportunity to sell low-cost goods and services that may not be profitable enough with traditional credit and debit, due to higher transaction costs. Others believe that cryptocurrency can provide new access to markets, including to individuals in the developing world who are not served by banks or other financial institutions. Cryptocurrency advocates also stress that the privacy associated with cryptocurrency, though raising significant challenges for law enforcement, can have valid and beneficial uses. For example, such advocates claim that greater anonymity may reduce the risk of account or identity theft associated with the use of traditional credit systems.

On the other hand, in addition to the substantial public safety and national security concerns discussed in this Framework, critics of cryptocurrency have raised questions about its supposed benefits. For example, certain critics contend that cryptocurrency could, if widely adopted, reduce the ability of national governments to regulate their economies through monetary policy. Others have raised concerns about the security of cryptocurrency wallets and exchanges, or pointed to the high volatility in value that most virtual currencies have experienced.

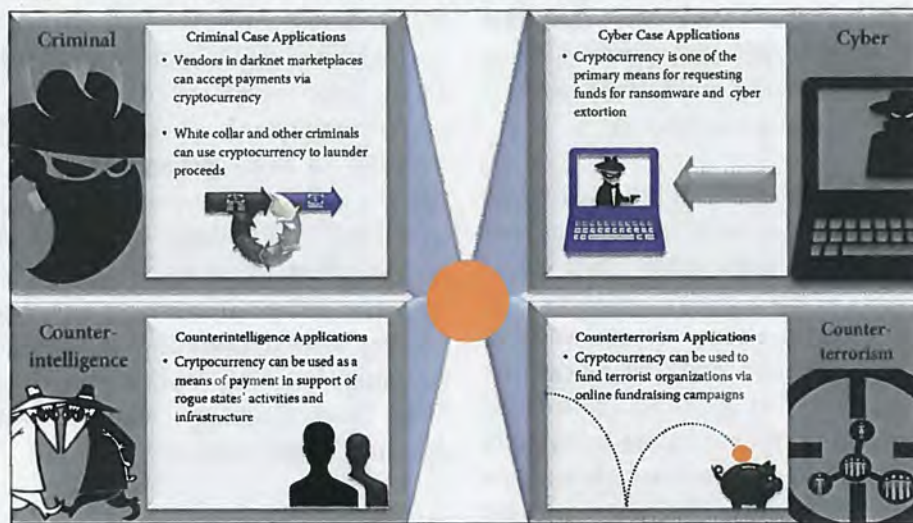
Whatever the overall benefits and risks of cryptocurrency, the Department of Justice seeks to ensure that uses of cryptocurrency are functionally compatible with adherence to the law and with the protection of public safety and national security.

## **C. Illicit Uses**

Many crimes that involve the use of cryptocurrency—for example, buying and selling illicit drugs—are not new, but criminals increasingly are leveraging cryptocurrency's features to advance and conceal unlawful schemes. In general, the illicit use of cryptocurrency can fall into three broad categories. As explained further below, bad actors may exploit cryptocurrency to: (1) engage in financial transactions associated with the commission of crimes, such as buying and selling drugs or weapons on the dark web, leasing servers to commit cybercrimes, or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) commit crimes directly



Figure 4 : Examples of Cryptocurrencies in Investigations



implicating the cryptocurrency marketplace itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors.<sup>6</sup>

### 1. Using Cryptocurrency Directly to Commit Crimes or to Support Terrorism

Criminals use cryptocurrency to facilitate crimes and to avoid detection in ways that would be more difficult with fiat currency or “real money.” They can avoid large cash transactions and mitigate the risk of bank accounts being traced, or of banks notifying governments of suspicious activity. Criminals have used cryptocurrency, often in large amounts and transferred across international borders, as a new means to fund criminal conduct ranging from child exploitation to terrorist fundraising. Cryptocurrency also has been used to pay for illegal drugs, firearms, and tools to commit cybercrimes, as well as to facilitate sophisticated ransomware and blackmail schemes.

**Buying and selling illegal things.** Criminals increasingly use cryptocurrency to purchase and to sell illicit items, such as drugs,<sup>7</sup> child sexual abuse material,<sup>8</sup> firearms, explosives, and toxic substances. There is also a robust market for counterfeit identification documents and for unlawfully obtained personal information, such as stolen credit card numbers. As discussed further below, purchases and sales of illegal goods and services using cryptocurrency often take place via dark web marketplaces created explicitly for the purpose of facilitating illicit transactions.<sup>9</sup>

**Buying and selling tools to commit crimes or to support terrorism.** Criminals and terrorists also use cryptocurrency to buy and sell “tools of the trade”—i.e., items that may or may not themselves be unlawful but are used for subsequent unlawful conduct. Such tools include raw materials to manufacture drugs or explosives, as well as cyber tools and computing capabilities (including servers and domains) to engage in cybercrime or to



conduct malign influence campaigns over social media. Criminals and terrorists have purchased these items and services using cryptocurrency, hoping that their activity and planning would go unnoticed.<sup>10</sup>

***Ransom, blackmail, and extortion.***

Increasingly, criminal extortion schemes are carried out in the digital space. Bad actors can use cryptocurrency as a payment method to facilitate ransom and blackmail without having to demand suitcases full of cash or risk bank accounts being traced. Moreover, criminals routinely infect victims' computers and servers with ransomware, which is a type of malicious software designed to encrypt or otherwise block access to valuable data until the victim agrees to provide a specified payment.<sup>11</sup> Criminals also demand payment after threatening to distribute confidential or embarrassing information (such as nude photos in cases of "sextortion") or engaging in "virtual kidnappings" where victims are misled into believing a loved one has been taken.

In April 2020, the Federal Bureau of Investigation ("FBI") issued an advisory about a potential increase in cryptocurrency fraud schemes due to the COVID-19 pandemic. The FBI noted that fraudsters were leveraging the fear and uncertainty caused by the pandemic to carry out scams in new ways. For example, some scammers threatened to infect victims and their families with coronavirus unless they sent payment in bitcoin. Others offered phony or defective products for sale using cryptocurrency with the promise that the products would cure or prevent the disease.<sup>12</sup>

***Raising funds for criminal and terrorist activity.*** Cryptocurrency technology also

has created new ways for criminal enterprises and terrorist organizations to raise funds. For example, as the notorious "Welcome to Video" case reveals, bitcoin has been used to monetize the production of child exploitation material—a development rarely seen before the rise of cryptocurrency. In addition to traditional fundraising, cryptocurrency also provides bad actors and rogue nation states with the means to earn profits directly by mining virtual currency, whether through legitimate mining operations or through illicit "cryptojacking" schemes, which are described further below.<sup>13</sup>

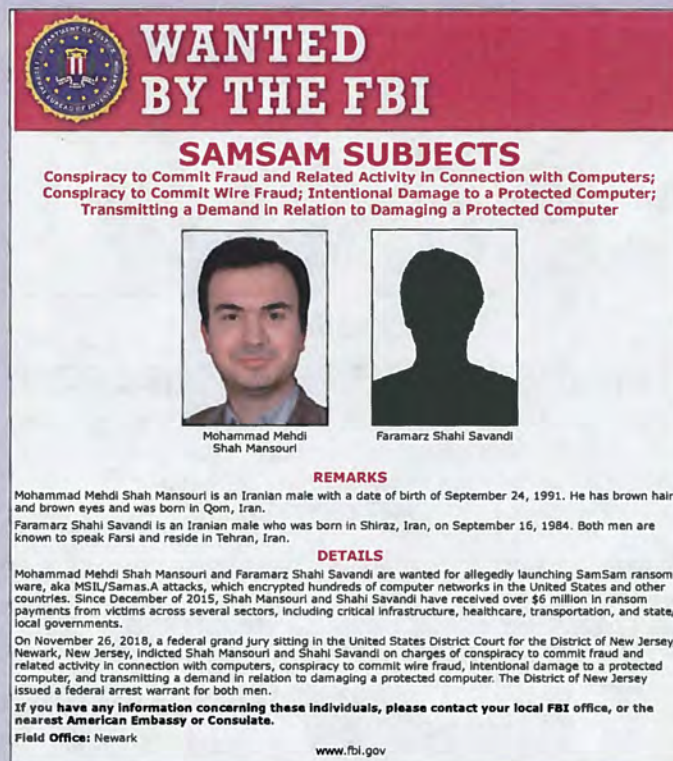
There is also evidence that certain terrorist groups are raising funds using cryptocurrency. While public data on terrorist use of cryptocurrency is limited, it is clear that terrorist networks have conducted fundraising operations through Internet-based crowdsourcing platforms in an attempt to evade stopgaps built into the international banking system.<sup>14</sup> In August 2015, for example, an individual was sentenced to over 11 years in federal prison for conspiring to provide material support and resources to the Islamic State of Iraq and al-Sham ("ISIS"), including by using social media to instruct donors on how bitcoin could provide untraceable financial support to terrorist groups.<sup>15</sup> More recently, in August 2020, the Department of Justice announced the government's largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing campaigns involving the al-Qassam Brigades ( Hamas's military wing), al-Qaeda, and ISIS. Each of those groups had used cryptocurrency technology and social media platforms to spread their influence and raise funds for terror campaigns.<sup>16</sup>



## SAMSAM

In a high-profile investigation into “21st-century digital blackmail,” a federal grand jury in November 2018 indicted two Iranian men for a 34-month-long international computer hacking and extortion scheme involving the deployment of the sophisticated “SamSam” ransomware.<sup>17</sup> According to the indictment, starting in December 2015, the defendants allegedly accessed victims’ computers, installed the SamSam ransomware, and then ran the program to encrypt critical data. The

defendants demanded ransom paid in bitcoin in exchange for the keys needed to decrypt the victims’ data. The defendants then allegedly exchanged the bitcoin proceeds into Iranian rial using Iran-based entities. All told, the defendants are alleged to have collected over \$6 million in ransom payments and to have caused over \$30 million in losses to more than 200 victims, which included hospitals, municipalities, and public institutions from around the world.



**WANTED BY THE FBI**

**SAMSAM SUBJECTS**

Conspiracy to Commit Fraud and Related Activity in Connection with Computers;  
Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer;  
Transmitting a Demand in Relation to Damaging a Protected Computer

**MOHAMMAD MEHDI SHAH MANSOURI**

**FARAMARZ SHAHI SAVANDI**

**REMARKS**

Mohammad Mehdi Shah Mansouri is an Iranian male with a date of birth of September 24, 1991. He has brown hair and brown eyes and was born in Qom, Iran.

Faramarz Shahi Savandi is an Iranian male who was born in Shiraz, Iran, on September 16, 1984. Both men are known to speak Farsi and reside in Tehran, Iran.

**DETAILS**

Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi are wanted for allegedly launching SamSam ransomware, aka MSIL/Samas.A attacks, which encrypted hundreds of computer networks in the United States and other countries. Since December of 2015, Shah Mansouri and Shahi Savandi have received over \$6 million in ransom payments from victims across several sectors, including critical infrastructure, healthcare, transportation, and state/local governments.

On November 26, 2018, a federal grand jury sitting in the United States District Court for the District of New Jersey, Newark, New Jersey, indicted Shah Mansouri and Shahi Savandi on charges of conspiracy to commit fraud and related activity in connection with computers, conspiracy to commit wire fraud, intentional damage to a protected computer, and transmitting a demand in relation to damaging a protected computer. The District of New Jersey issued a federal arrest warrant for both men.

**If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.**

Field Office: Newark

www.fbi.gov

**Figure 5: The “SamSam” Ransomware Attack –  
An Example of 21st Century Digital Blackmail**



## WELCOME TO VIDEO

On October 16, 2019, the Department of Justice announced the indictment and arrest of the alleged operator of Welcome to Video, a darknet child pornography website that was the world's largest online child sexual exploitation market at the time of its seizure. Welcome to Video allegedly offered child sexual exploitation photos and videos for sale using bitcoin, and relied on virtual currency accounts to fund the site and to promote further exploitation of children. The site allegedly hosted approximately eight terabytes of child sexual exploitation material—including over 250,000 unique videos—and claimed over one million downloads of exploitative material by its users. In addition to the operator, at least 337 users of the site have been arrested and charged across the United States and around the world. The globally coordinated law enforcement operation targeting Welcome to Video and its users led to the rescue of at least 23 minor victims who were actively being abused, allegedly by the site's users.<sup>18</sup>



Figure 6: Welcome to Video Website after Seizure by the Government



## DARKSCANDALS

A spin-off of the “Welcome to Video” investigation, the Department of Justice on March 12, 2020 announced the indictment of a Dutch national for his alleged operation of DarkScandals, a website that featured violent rape videos and depictions of child sexual abuse. According to the indictment, DarkScandals hosted over 2,000 videos and images advertised as including “real blackmail, rape and forced videos of girls all around the world.”<sup>19</sup> Users could allegedly access the illicit content by paying cryptocurrency or by uploading new content depicting rape or other sexual abuse. The site’s alleged operator was charged with distribution of child pornography; production and transportation of obscene matters for sale or distribution; engaging in the business of selling or transferring obscene matter; and money laundering. In addition, the government filed a civil forfeiture action seeking recovery of illicit funds from 303 virtual currency accounts allegedly used by customers to fund DarkScandals and to promote child exploitation.<sup>20</sup>

Case 1:20-cv-00712 Document 1 Filed 03/12/20 Page 1 of 32	
UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA	
UNITED STATES OF AMERICA,	)
Plaintiff,	)
v.	)
THREE HUNDRED THREE VIRTUAL CURRENCY ACCOUNTS,	)
THE DARKSCANDALS.COM DOMAIN,	)
— and —	)
THE DARKSCANDALS.CO DOMAIN,	)
Defendants.	)
Civil Action No. 20-cv-712	
<u>VERIFIED COMPLAINT FOR FORFEITURE <i>IN REM</i></u>	
COMES NOW, Plaintiff the United States of America, by and through the United States Attorney for the District of Columbia, and brings this Verified Complaint for Forfeiture <i>In Rem</i> against the defendant properties, namely: 303 virtual currency accounts, the darkscandals.com domain, and the darkscandals.co domain (collectively, the “Defendant Properties”), which are listed in Attachment A. The United States alleges as follows in accordance with Rule G(2) of the Federal Rules of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions.	
<u>THE DEFENDANT PROPERTIES</u>	
1 The Defendant Properties are comprised of miscellaneous financial instruments in 303 virtual currency exchange accounts at eight different virtual currency exchanges (listed below), and two domain names: darkscandals.com and darkscandals.co	

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA	
Holding a Criminal Term Grand Jury Sworn in May 7, 2019	
UNITED STATES OF AMERICA	1 Case: 20-cr-0065
v.	1 Assigned To: Judge Dabney L. Friedrich
MICHAEL RAHIM MOHAMMAD,	1 Assign. Date: 3/5/2020
Defendant.	1 Description: INDICTMENT (B)
	1 Related Case No. 18CR243 (DLF)
	1 18 U.S.C. § 2252(a)(2)
	1 (Distribution of Child Pornography)
	1 18 U.S.C. § 1465
	1 (Production and Transportation of
	1 Obscene Matters For Sale or
	1 Distribution)
	1 18 U.S.C. § 1466
	1 (Engaging In The Business of Selling or
	1 Transferring Obscene Matter)
	1 18 U.S.C. § 1956(a)(2)(A)
	1 (Laundering of Monetary Instruments)
	1 FORFEITURE:
	1 21 U.S.C. § 853; 18 U.S.C. § 982;
	1 18 U.S.C. § 1467 and 2253
	1 <u>UNDER SEAL</u>

**Figure 7: The Indictment and Civil Forfeiture Papers Filed by the Government in the DarkScandals Matter**



## DISMANTLING OF TERRORIST FINANCING CAMPAIGNS

On August 13, 2020, the Department of Justice announced the dismantling of three terrorist financing cyber-enabled campaigns involving the al-Qassam Brigades, al-Qaeda, and ISIS. Investigation revealed that these terrorist groups used sophisticated cyber-tools to assist in financing their operations, including through online solicitation of cryptocurrency donations from supporters around the world. The government has filed three civil forfeiture complaints and a criminal complaint involving the seizure of four websites, four Facebook pages, over 300 cryptocurrency accounts, and millions of dollars.

***Al-Qassam Brigades.*** According to the government's complaint, the al-Qassam Brigades posted requests for bitcoin donations on its social media page and official websites, claiming that such donations would be untraceable and used to support violent causes. The group's websites included videos on how to make anonymous donations using unique bitcoin addresses. Fortunately, IRS, HSI, and FBI personnel were able to track and seek forfeiture of the 150 cryptocurrency accounts used to launder funds to and from the al-Qassam Brigades' accounts.

***Al-Qaeda.*** The government's investigation also revealed that al-Qaeda and affiliated terrorist groups operated a bitcoin money laundering network using social media platforms and encrypted messaging apps to solicit cryptocurrency donations. In some cases, the groups claimed to be acting as charities, while actually soliciting funds for violent terrorist attacks. Al-Qaeda and their affiliates used sophisticated techniques in an attempt to conceal their fundraising efforts, but law enforcement was able to identify and seek forfeiture of 155 virtual currency assets linked to the groups.

***ISIS.*** Finally, the government's investigation uncovered a scheme whereby individuals associated with ISIS marketed fake personal protective equipment ("PPE")—such as N95 respirator masks—to customers across the globe in an effort to take advantage of the COVID-19 pandemic. The funds from such sales would have been used to support ISIS's operations.<sup>21</sup>

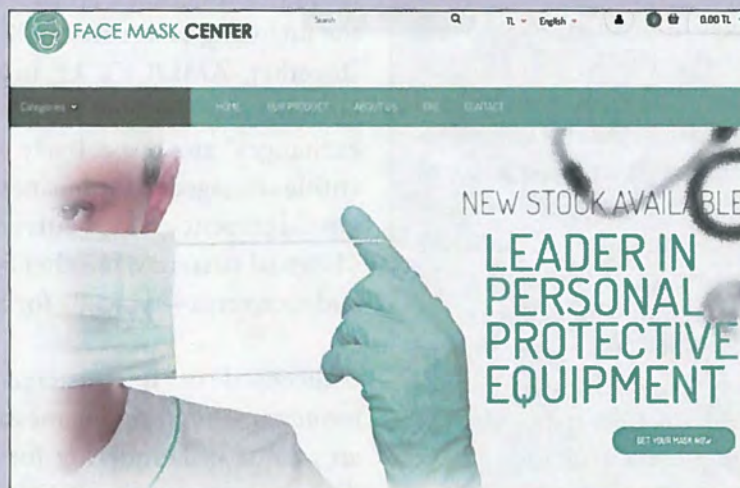


**Figure 8: “Donate Anonymously with Cryptocurrency” – An al-Qaeda-Affiliated Group Seeks Anonymous Donations in Bitcoin**



*The group that posted the request for donations claimed to be a Syrian charity, but allegedly sought funds to support “the mujahidin in Syria with weapons, financial aid and other projects assisting the jihad.”<sup>22</sup>*

**Figure 9: Website Maintained by an ISIS Facilitator to Sell Fake PPE**





## 2. Using Cryptocurrency to Hide Financial Activity

In addition to being used directly in transactions to commit crime or to support terrorism, bad actors also use cryptocurrency to hide and to promote financial activities attendant to unlawful conduct.

**Money laundering.** Criminals of all types are increasingly using cryptocurrency to launder their illicit proceeds. Broadly speaking, money laundering occurs when an individual knowingly conducts a financial transaction connected to or stemming from a criminal offense in order to promote the

offense, conceal the proceeds, or evade federal reporting requirements.<sup>24</sup> Such conduct can be substantially easier when the movement of funds takes place online and anonymously, involving the exchange of cryptocurrency for other forms of cryptocurrency or the conversion of cryptocurrency to fiat currency. Indeed, the explosion of online marketplaces and exchanges that use cryptocurrency may provide criminals and terrorists with new opportunities to transfer illicitly obtained money in an effort to cover their financial footprints and to enjoy the benefits of their illegitimate earnings. Transnational criminal organizations, including drug cartels, may find cryptocurrency especially useful to hide financial activities and to move vast sums of money efficiently across borders without detection.

### BITCOIN MAVEN

In July 2018, Theresa Tetley, known by her online moniker “Bitcoin Maven,” was sentenced to one year in federal prison for money laundering and for operating an unlicensed bitcoin-for-cash money-transmitting business. Through her unregistered bitcoin exchange business, Tetley facilitated money laundering by providing money-transmission services to members of the public, including at least one individual who received bitcoin from the sale of drugs on the dark web. Tetley also conducted an exchange of bitcoin for cash with an undercover agent who represented that his bitcoin were the proceeds of narcotics trafficking. In sentencing documents, the government revealed that Tetley’s business “fueled a black-market financial system” that “purposely and deliberately existed outside of the regulated bank industry.”<sup>23</sup>

**Operating unlicensed, unregistered, or non-compliant exchanges.** Criminals may also attempt to hide financial activity by using cryptocurrency exchanges that do not comply with internationally recognized anti-money laundering (“AML”) and combating the financing of terrorism (“CFT”) standards (together, “AML/CFT”).<sup>25</sup> In general, “virtual currency exchangers” and “virtual currency exchanges” are, respectively, individuals and entities engaged in the business of exchanging virtual currency for fiat currency, other forms of virtual currency, or other types of assets—and vice versa—typically for a commission.<sup>26</sup>

Unlicensed or unregistered exchanges or money transmitting businesses can “provide an avenue of laundering for those who use digital currency for illicit purposes.”<sup>27</sup> In



### BTC-e

In 2017, prosecutors in the United States announced the indictment of the virtual currency exchange “BTC-e” and of one of the exchange’s principal operators. BTC-e received more than \$4 billion worth of bitcoin over the course of its operation. According to the indictment, to appeal to criminals as a customer base, BTC-e did not require users to validate their identities, obscured and anonymized transactions and sources of funds, and lacked appropriate anti-money laundering processes. As a result, the exchange predictably served as a hub for international criminals seeking to hide and launder ill-gotten gains. The indictment alleges that BTC-e facilitated transactions for cybercriminals worldwide and received criminal proceeds from numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings. The Department of Justice filed criminal charges, and the Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”) assessed a \$110 million civil penalty against the exchange for willfully violating U.S. anti-money laundering laws, and a \$12 million penalty against the exchange’s operator personally.<sup>28</sup> BTC-e is only one example in a series of cases in which the Department of Justice has pursued criminal charges against cryptocurrency exchanges for operating as unlicensed money services businesses.<sup>29</sup>

addition, even properly registered exchanges can serve as a haven for criminal activity by operating under lax rules or by flouting AML protocols. In the normal course, registered exchanges that comply with AML standards and “know your customer” (“KYC”) requirements are likely to possess relevant transactional information. However, exchanges that avoid compliance with such requirements provide criminals and terrorists with opportunities to hide their illicit financial activity from regulators and investigators. Moreover, as discussed in Part II.C below, the requirements for exchanges to register, obtain licenses, and collect information about customers and their transactions are not consistent across international jurisdictions. This inconsistency can create challenges for international law enforcement and regulatory agencies operating in this space.

**Evading taxes.** As with money laundering, the potential difficulties in tracking cryptocurrency transactions can also facilitate tax evasion. Because of these difficulties, tax cheats may believe that the Internal Revenue Service is not able to uncover or attribute their cryptocurrency transactions, and they may even use additional anonymizing features of cryptocurrencies to further obfuscate their transactions. Tax cheats may then attempt tax evasion by, among other things, not reporting capital gains from the sale or other disposition of their cryptocurrency, not reporting business income received in cryptocurrency, not reporting wages paid in cryptocurrency, or using cryptocurrency to facilitate false invoice schemes designed to fraudulently reduce business income.<sup>30</sup> Importantly, the tax loss from unreported capital gains can



be significant as cryptocurrencies emerge and fluctuate in the market. For example, the value of one bitcoin famously rose from around \$1,000 to around \$20,000 in 2017, as investors rushed to that cryptocurrency as an investment vehicle.

**Avoiding sanctions.** Finally, individuals, companies, and rogue regimes may use cryptocurrency in attempt to avoid the reach of economic sanctions imposed by the United States or other rule-of-law countries. Cryptocurrency's decentralized and peer-to-peer format may allow sanctioned entities to bypass the financial controls built into traditional financial marketplaces to enforce such sanctions. Indeed, public reports note that several nations have explored the creation and use of their own state-sponsored cryptocurrencies, which could serve as a platform to evade financial controls and oversight. As explained by the U.S. Department of the Treasury, for example, Venezuela attempted to launch a national cryptocurrency—called the “Petromoneda” or “Petro”—in the “hope that the [cryptocurrency] would allow Venezuela to circumvent U.S. financial sanctions.”<sup>31</sup> Other countries, including Russia and Iran, have threatened to use existing cryptocurrencies to dodge sanctions or to develop their own cryptocurrencies specifically to avoid international oversight.<sup>32</sup>

### **3. Committing Crimes within the Cryptocurrency Marketplace Itself**

In addition to offering a means to commit old crimes in new ways, cryptocurrencies and the platforms on which they operate have often

themselves become the target of criminal activity. To protect future victims, as well as to safeguard the integrity of cryptocurrency technology, more must be done to promote security and combat criminal activity on digital exchanges and platforms.

**Theft and fraud.** Cryptocurrency's features, as well as the overall “opaqueness and lack of transparency in the cryptocurrency market,”<sup>33</sup> make it particularly attractive, adaptable, and scalable as a target for theft. Criminals—and even rogue state actors<sup>34</sup>—can steal cryptocurrency by exploiting security vulnerabilities in wallets and exchanges. Thieves can hack wallets and exchanges directly; employ social engineering and other tools to obtain passwords and PINs from unsuspecting users; or, if they themselves operate exchanges, engage in insider theft. Public reports estimate that at least \$1.7 billion of cryptocurrency was stolen or scammed in 2018, with over \$950 million of that amount stolen from cryptocurrency exchanges. In 2019, over \$4.5 billion of cryptocurrency reportedly was lost to theft or fraud, more than doubling the losses from the prior year.<sup>35</sup> This susceptibility to theft on a massive scale demonstrates that the lack of appropriate regulation and monitoring of cryptocurrency exchanges poses a threat to cryptocurrency users themselves, as well as to the general public.

In addition to digital theft, fraudsters use cryptocurrency to bilk unsuspecting investors, to promote scams, and to engage in market manipulation. For example, in July 2018, Jon E. Montroll pleaded guilty to securities fraud and to obstruction of



justice related to his operation of two online Bitcoin services: WeExchange Australia, Pty. Ltd., a Bitcoin depository and currency exchange service, and BitFunder.com, which facilitated the purchase and trading of virtual shares of business entities that listed shares on the platform. Montroll pleaded guilty to converting a portion of WeExchange users' bitcoin to his personal use without the users' knowledge or consent. Montroll also admitted failing to disclose a hack of the BitFunder programming code that caused the platform to credit hackers with profits they did not earn, thereby enabling the hackers to wrongfully withdraw approximately 6,000 bitcoin. The hack meant that Montroll lacked the bitcoin necessary to cover what he owed to investors. Despite this, and as a result of his omissions and misrepresentations, Montroll still raised approximately 978 bitcoin after the discovery of the hack. In addition to committing securities fraud, Montroll provided a falsified screenshot and false and misleading answers to Securities and Exchange Commission ("SEC") personnel during the course of their investigation.<sup>36</sup>

In another fraudulent scheme involving cryptocurrency, Joseph Kim was sentenced in November 2018 to 15 months in federal prison for misappropriating \$1.1 million in bitcoin and litecoin. Kim worked as an assistant trader for a Chicago trading firm that had formed a cryptocurrency group to engage in trading of virtual currencies. Over a two-month period in 2017, Kim misappropriated at least \$600,000 of his trading firm's bitcoin and litecoin cryptocurrency for his own personal benefit, and made false statements and representations

to the company's management to conceal the theft. Subsequently, Kim engaged in another scheme in which he incurred \$545,000 in losses by trading cryptocurrencies using funds that he solicited from friends through lies.<sup>37</sup>

**Cryptojacking.** The ability to digitally mine cryptocurrency provides criminals an independent reason to hack into and co-opt computers belonging to unsuspecting individuals and organizations. The unauthorized use of someone else's computer to generate (or "mine") cryptocurrency is called "cryptojacking."<sup>38</sup> This is often accomplished through the use of malware or compromised websites, which cause the victim's computer to run crypto-mining code. Considering the value of cryptocurrency compared to the relative ease of secretly using a victim's computer, cryptojacking is another relatively low-risk but high-reward illegal activity made possible by cryptocurrency technology. Reports indicate that rogue states, such as North Korea, have explored using malware to mine cryptocurrency illicitly.<sup>39</sup>

#### **D. The Role of Darknet Markets**

Many of the cryptocurrency-related crimes described above are made possible through the operation of online black markets on the dark web. Indeed, much of the illicit conduct involving cryptocurrency occurs via darknet websites and marketplaces that allow criminals around the world to connect in unregulated virtual bazaars with a great deal of anonymity. These illicit marketplaces offer the opportunity not only to buy and to



## OPERATION DISRUPTOR

In September 2020, the Department of Justice joined Europol to announce the results of Operation Disruptor, a coordinated international effort to disrupt opioid trafficking on the dark web. The extensive operation lasted nine months and was conducted across the United States and Europe, demonstrating international law enforcement's continued partnership against the illegal sale of drugs and other illicit goods and services.

Following the Wall Street Market takedown in May 2019, U.S. and international law enforcement agencies obtained intelligence to identify dark web drug traffickers, resulting in a series of complementary, but separate, law enforcement investigations. Operation Disruptor actions have resulted in the arrest of 179 dark web drug traffickers and fraudulent criminals who engaged in tens of thousands of sales of illicit goods and services across the United States and Europe.

This operation resulted in the seizure of over \$6.5 million in both cash and virtual currencies; approximately 500 kilograms of drugs worldwide; 274 kilograms of drugs, including fentanyl, oxycodone, hydrocodone, methamphetamine, heroin, cocaine, ecstasy, MDMA, and medicine containing addictive substances in the United States; and 63 firearms.

Operation Disruptor led to 121 arrests in the United States including two in Canada at the request of the United States, 42 in Germany, eight in the Netherlands, four in the United Kingdom, three in Austria, and one in Sweden. A number of investigations are still ongoing to identify the individuals behind dark web accounts. Operation Disruptor illustrates the investigative power of federal and international partnerships to combat the borderless nature of online criminal activity, including activity using cryptocurrency.





## DEEPPDOTWEB

In May 2019, the Department announced the indictment of the alleged owners and operators of the website known as DeepDotWeb (“DDW”) on charges of money laundering conspiracy. According to the indictment, DDW served as a gateway that provided users with access to numerous darknet marketplaces offering for sale illegal narcotics (including fentanyl, heroin, and crystal meth), firearms, malicious software, hacking tools, stolen credit card information, and other contraband. The owners of DDW allegedly received payments—styled as “referral bonuses”—paid in virtual currency to a DDW-controlled bitcoin wallet from individuals who used the site to purchase illicit items. DDW’s owners allegedly attempted to conceal the nature of these illegal payments, which totaled more than \$15 million, by transferring the bitcoin they received to other bitcoin addresses and to bank accounts opened under the names of shell companies. During the course of the conspiracy, DDW’s owners are alleged to have referred hundreds of thousands of users to darknet marketplaces, including AlphaBay, Agora Market, Abraxas Market, Dream Market, Valhalla Market, Hansa Market, TradeRoute Market, Dr. D’s, Wall Street Market, and Tochka Market. In turn, these users completed hundreds of millions of dollars’ worth of allegedly illicit transactions.<sup>40</sup>

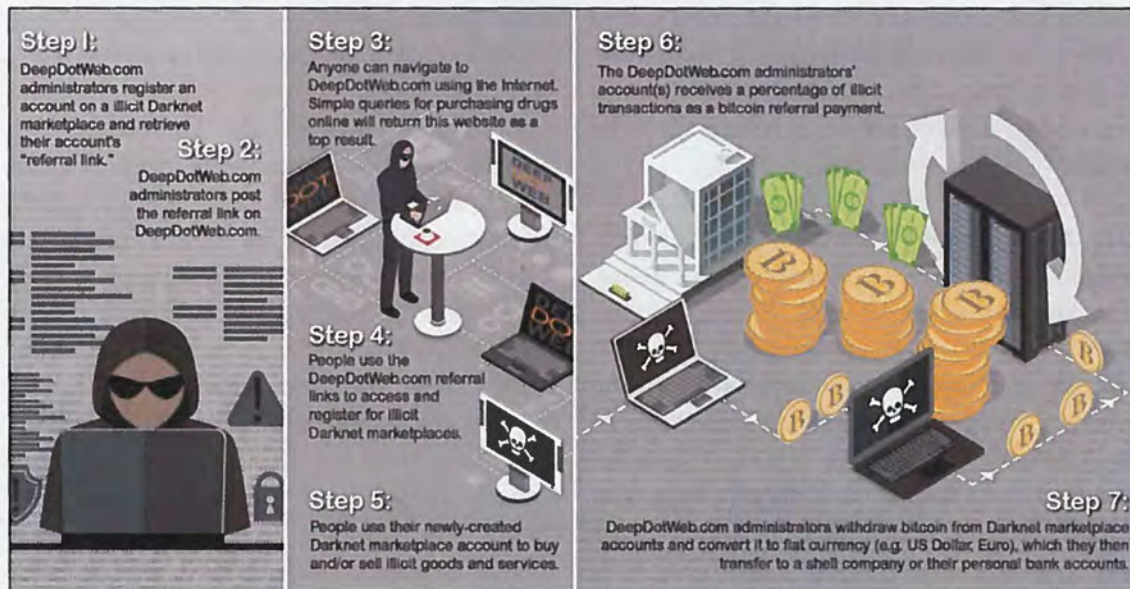


Figure 10: Anatomy of the DeepDotWeb Criminal Operation



## DREAM MARKET

In October 2018, an administrator of the darknet marketplace Dream Market was sentenced to 20 years in federal prison for narcotics trafficking and money laundering. The defendant, Gal Vallerius, initially participated in the marketplace as a vendor, selling Oxycodone and Ritalin. He later acted as an administrator and senior moderator, supporting



illicit narcotics and money laundering transactions between the site's buyers and vendors. Following the dismantling of Silk Road and AlphaBay, Dream Market had become one of the largest darknet criminal marketplaces, and all of its items and services were offered for sale in exchange for bitcoin or other peer-to-peer cryptocurrencies.

sell illegal goods and tools for committing crimes, but also to launder money and to hide ill-gotten gains. As a result, darknet markets are a natural place for cryptocurrency to be widely used and exploited.

One of the most notorious online darknet websites, which relied exclusively on bitcoin, was known as Silk Road. Prior to being dismantled by law enforcement in 2013, Silk Road served as an extensive online criminal marketplace used by thousands of drug dealers and other vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers. Silk Road was also used to launder hundreds of millions of dollars in illicit proceeds. When the site was

shut down, other cryptocurrency-reliant darknet marketplaces sprung up in its place. Working closely with its international law enforcement partners, the Department of Justice's efforts to dismantle these virtual black markets continue in earnest, including the successful disruption of the notorious AlphaBay and Hansa marketplaces in July 2017; the Wall Street Market ("WSM") and DeepDotWeb ("DDW") websites in May 2019;<sup>41</sup> and the coordinated takedowns of darknet markets dedicated to opioid trafficking reflected in Operation SaboTor (March 2019)<sup>42</sup> and Operation Disruptor (September 2020).<sup>43</sup> Cryptocurrencies played a central facilitating role in each of these global criminal enterprises. For example, as the Department announced at



the time that indictments were returned against the alleged owners and operators of DDW, “Between in and around November 2014 and April 10, 2019, DDW received approximately 8,155 bitcoin in kickback payments from darknet marketplaces, worth approximately \$8,414,173 when adjusted for the trading value of bitcoin at the time of each transaction.”<sup>44</sup> Attesting to the complexity of these illicit cross-border payments, many of which took place entirely outside of the established international banking network, the bitcoin was transferred to DDW’s bitcoin wallet, which the defendants are alleged to have controlled, in a series of “more than 40,000 deposits,” and was subsequently withdrawn to various destinations (both known and unknown) around the world through over 2,700 transactions.<sup>45</sup>

## II. Law and Regulations

As discussed in Part I, a wide range of criminal activity may involve or be facilitated by the use of cryptocurrency. On numerous occasions, the Department of Justice has used available legal tools to pursue successful prosecutions of such activity. This Part provides an overview of the legal authorities the Department uses to prosecute those who misuse cryptocurrency, and describes the roles and responsibilities of the Department’s key government partners.

### A. Criminal Code Authorities

As discussed above, cryptocurrency is often the preferred payment method for the distribution of contraband and of other illegal goods and services, and it can be used

to collect funds from victims of traditional fraud or computer intrusions. A wide variety of federal charges can be brought to bear for such conduct, including, for example:

- **Wire fraud**, 18 U.S.C. § 1343. (For examples of cryptocurrency prosecutions involving the wire fraud statute, see the indictment of AriseBank CEO Jared Rice, Sr., discussed on pages 31-32, and the indictment of two Iranian men for deployment of SamSam ransomware, discussed on pages 8 and 26.)

- **Mail fraud**, 18 U.S.C. § 1341.

- **Securities fraud**, 15 U.S.C. §§ 78j and 78ff. (For example, see the indictment of AriseBank CEO Jared Rice, Sr., discussed on pages 31-32, and the indictment of Jon E. Montroll, discussed on pages 15-16.)

- **Access device fraud**, 18 U.S.C. § 1029. (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)

- **Identity theft and fraud**, 18 U.S.C. § 1028. (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)

- **Fraud and intrusions in connection with computers**, 18 U.S.C. § 1030. (For example, see the indictment of two Iranian men for deployment of SamSam ransomware, discussed on pages 8 and 26.)

- **Illegal sale and possession of firearms**, 18 U.S.C. § 921 *et seq.*

- **Possession and distribution of counterfeit items**, 18 U.S.C. § 2320.



- **Child exploitation activities**, 18 U.S.C. § 2251 *et seq.* (For example, see the indictment of Ammar Atef Alahdali, discussed on page 6, footnote 8.)
- **Possession and distribution of controlled substances**, 21 U.S.C. § 841 *et seq.* (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)
- **Operation of an unlicensed money transmitting business**, 18 U.S.C. § 1960 (For example, see the indictment of BTC-e and its operator, discussed on pages 14 and 46, and the indictment of two Chinese nationals, discussed on pages 27-28.)
- **Failure to comply with Bank Secrecy Act requirements**, 31 U.S.C. § 5331 *et seq.*

The Department also can bring to bear a wide variety of money laundering charges in cases involving misuse of cryptocurrency. Depending on the facts and circumstances, transactions involving cryptocurrency can form the basis of concealment, promotion, sting, and international money laundering violations. In addition, individuals and companies engaged in money transmission involving virtual assets, referred to below as “virtual asset service providers,” may be subject to, and may fail to comply with, both federal and State registration, record keeping, and reporting requirements. Potential charges include, for example:

- **Money laundering**, 18 U.S.C. § 1956 *et seq.* (For examples of cryptocurrency prosecutions involving the federal money laundering statute, see the indictment of BTC-e and its operator, discussed on pages 14 and 46; the indictment of AlphaBay, discussed on pages 19 and 47; the indictment of a Dutch national for his operation of DarkScandals, discussed on page 10; and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Transactions involving proceeds of illegal activity**, 18 U.S.C. § 1957. (For example, see the indictment of BTC-e and its operator, discussed on pages 14 and 46.)

Virtual asset transactions may also form the basis for prosecution if, for example, they are used as a means to provide material support or resources to terrorists or foreign terrorist organizations.<sup>46</sup> Such transactions could also be used for payments that facilitate other crimes implicating national security, such as espionage<sup>47</sup> or conspiracies involving interference in the political process, in violation of various federal laws.

Finally, the Department frequently uses existing criminal authorities to seize and forfeit virtual assets and other property derived from or involved in activity of an individual or organization charged with a crime. The Department also uses available civil authorities for such seizures and forfeitures, which allow the government to “arrest” the assets themselves, even in cases where no person is charged criminally or where a defendant may not be prosecutable due to, for example, death or flight from a jurisdiction. Statutory authorities for forfeiture include:

- **Criminal forfeiture**, 18 U.S.C. § 982; 21 U.S.C. § 853. (For examples of cryptocurrency prosecutions involving the criminal forfeiture statute, see the indictment



of the alleged administrator of Helix, discussed on page 43, and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Civil forfeiture**, 18 U.S.C. § 981. (For example, see the verified complaints in the AlphaBay case, discussed on pages 9 and 47; the Welcome to Video case, discussed on pages 7 and 9; the DarkScandals case, discussed on page 10; the cases involving the al-Qassam Brigades, al-Qaeda, and ISIS, discussed on pages 7 and 11-12; and the cases involving hacks of virtual currency exchanges by North Korean actors, discussed on pages 27 and 28.)

## B. Regulatory Authorities

As described above, the Department of Justice has broad and diverse federal jurisdiction over criminal and other improper conduct that may involve cryptocurrency and other types of virtual assets. A number of regulatory agencies in the United States also have authority to enforce statutes and regulations that apply to various virtual-asset-related activities. The Department has worked closely and cooperatively with these agencies in identifying and proceeding against individuals who misuse cryptocurrency for illicit purposes.

Much of the regulatory activity conducted by the agencies discussed below focuses on money services businesses (“MSBs”) and virtual asset service providers (“VASPs”). In general, MSBs are individuals or entities in one or more of the following capacities:

- i. currency dealer or exchanger;
- ii. check casher;
- iii. issuer of traveler’s checks, money orders, or stored value;
- iv. seller or redeemer of traveler’s checks, money orders, or stored value;
- v. money transmitter; or
- vi. the U.S. Postal Service.<sup>48</sup>

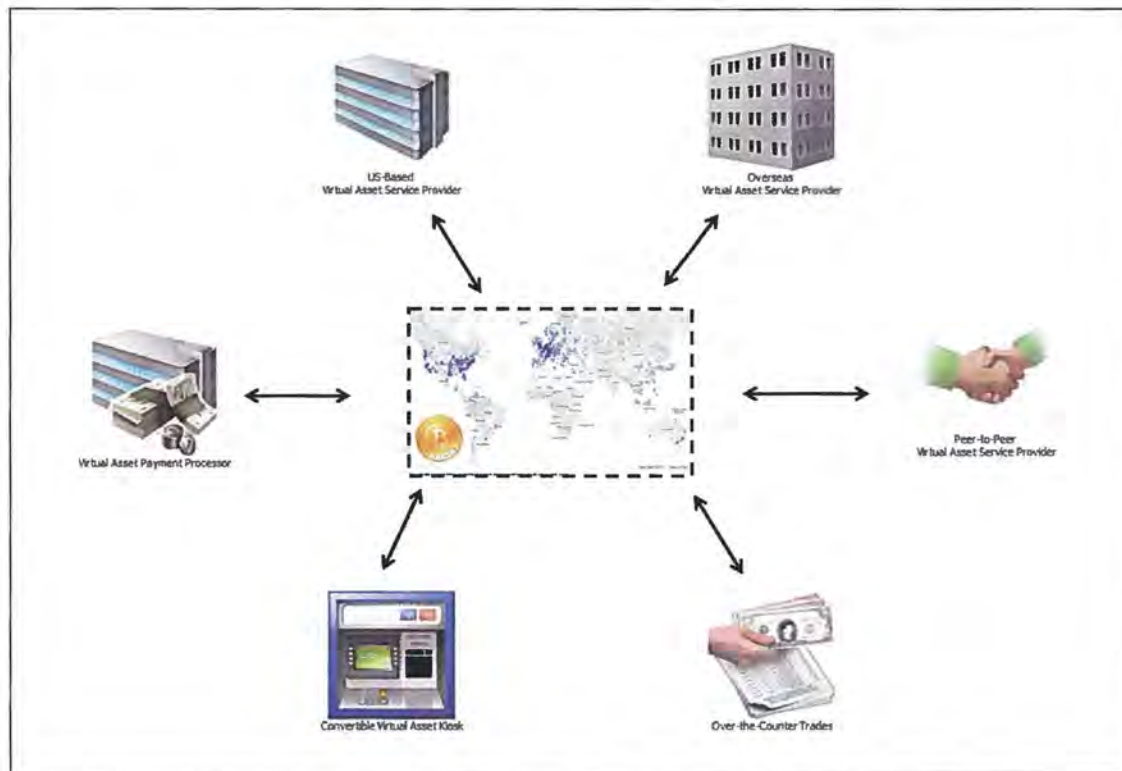
VASPs are individuals or entities operating as a business to conduct one or more of the following activities for or on behalf of another entity or individual:

- i. exchanges between virtual assets and fiat currencies;
- ii. exchanges between one or more forms of virtual assets;
- iii. transfers of virtual assets;
- iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or
- v. participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.<sup>49</sup>

In the United States, individuals and entities that offer money transmitting services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs. Like brick-and-mortar financial institutions, MSBs are subject to AML/CFT<sup>50</sup> regulations as well as certain licensing and registration requirements, as discussed below.



**Figure 11: Depiction of the Operation of a Global Virtual Asset Network**



### 1. The Financial Crimes Enforcement Network and the Bank Secrecy Act

**Regulatory authority.** MSBs, including cryptocurrency exchanges, function as regulated businesses subject to the federal Bank Secrecy Act (“BSA”).<sup>51</sup> The U.S. Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”) has primary responsibility for administering the BSA and for implementing its regulations.<sup>52</sup> Part of that responsibility includes maintaining the BSA database, which is a repository of reports about financial transactions that are potentially indicative of money laundering.<sup>53</sup> FinCEN serves as the Financial Intelligence Unit (“FIU”) for the United States, meaning it is the central entity responsible for receiving and analyzing suspicious transaction reports and other information concerning money laundering, financing of terrorism, and related offenses.<sup>54</sup> FinCEN regulates individuals and entities engaged in the business of accepting and transmitting convertible virtual currency (“CVC”), which refers to “virtual currency

that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of ‘value that substitutes for currency.’”<sup>55</sup> In 2011, FinCEN issued a final rule that, among other things, defined “money transmission services” to include accepting and transmitting “currency, funds, or *other value that substitutes for currency* by any means.”<sup>56</sup> The phrase “other value that substitutes for currency” was intended to cover situations where a transmission includes something that the parties recognize has value that is equivalent to, or can substitute for, fiat currency.<sup>57</sup> The definition of “money transmission” is technology-neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another, or from one location to another, is regulated under the BSA.

To provide additional clarity and to respond to questions from the private sector, FinCEN issued interpretive guidance in March 2013 and in May 2019 regarding the application of its regulations to certain transactions involving the acceptance of currency or funds and the transmission of virtual currency.<sup>58</sup> The 2013 FinCEN guidance identified the participants in some virtual currency arrangements, including “exchangers,” “administrators,” and “users,” and clarified that while exchangers and administrators generally qualify as money transmitters under the BSA, users do not.<sup>59</sup> The guidance also stated that virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered MSBs to the extent they accept

and transmit CVC or when they buy or sell CVC for any reason.<sup>60</sup> As MSBs, such virtual currency administrators and exchangers are obliged to have AML programs, to file Suspicious Activity Reports (“SARs”), and to follow other BSA requirements.<sup>61</sup>

The May 2019 FinCEN guidance addressed how FinCEN regulations relating to MSBs apply to various business models involving money transmission denominated in CVC, including with reference to prior administrative rulings.<sup>62</sup> Importantly, the guidance discussed the application of the BSA to foreign-located MSBs, individual peer-to-peer exchangers, wallet providers, cryptocurrency kiosk operators, CVC-to-CVC transactions, payment processors, mixers and tumblers, initial coin offerings, Internet casinos, trading platforms, decentralized exchanges and distributed applications (“DApps”), miners, software providers, and developers of such technologies. In particular, the guidance outlined the application of FinCEN’s regulations to persons who provide anonymizing services or who are engaged in activities involving anonymity-enhanced CVCs. According to FinCEN, anonymizing service providers and some AEC issuers are money transmitters, whereas an individual or entity that merely provides anonymizing software is not.

FinCEN has stated that MSBs that conduct money transmission in CVCs must meet the same AML/CFT standards as other MSBs under the Bank Secrecy Act. This includes registering with FinCEN, establishing an AML program reasonably designed to prevent



money laundering and terrorist financing, and meeting certain record keeping and reporting obligations, such as filing SARs.<sup>63</sup> SARs and currency transaction reports (“CTRs”) are a vital source of information that all MSBs—including VASPs, when applicable—should be generating where appropriate, and filing with FinCEN. These reports may contain leads for law enforcement and information necessary to deter, investigate, and prosecute criminal activity.

Importantly, FinCEN’s requirements apply equally to domestic and foreign-located MSBs—even if the foreign-located MSB does not have a physical presence in the United States.<sup>64</sup> The MSB need only do business in whole or substantial part in the United States. In addition, parties become money transmitters, and therefore MSBs, whether they exchange from fiat to convertible virtual currency or from one virtual currency to another virtual currency.<sup>65</sup>

***Interaction with the Department of Justice.*** FinCEN’s relationship with the Department of Justice and other law enforcement agencies generally falls into two categories: crime prevention (through compliance requirements that prevent money laundering and terrorist activity) and investigatory assistance (through, for example, the provision of leads for criminal investigations generated by regulatory reporting requirements regarding suspicious activity). In addition, FinCEN has the ability to share and to receive financial intelligence information among foreign counterparts, thus creating an important

international network. FinCEN also has civil enforcement authority through which it can impose monetary penalties to supplement, or as an alternative to, criminal prosecution in appropriate circumstances, and can take regulatory action to address money laundering and terror financing concerns raised in the virtual currency space.<sup>66</sup>

In just one example of successful collaboration, FinCEN, working in coordination with the United States Attorney’s Office for the Northern District of California, assessed a \$700,000 civil monetary penalty in 2015 against Ripple Labs Inc. and its wholly-owned subsidiary, XRP II, LLC.<sup>67</sup> Ripple Labs, which is headquartered in San Francisco, facilitated transfers of virtual assets and provided virtual asset exchange transaction services. The company also operated a virtual currency known as XRP that, in 2015, was the second-largest cryptocurrency by market capitalization after Bitcoin. Parallel investigations by the Department of Justice and FinCEN found that Ripple Labs willfully violated several requirements of the BSA by acting as an MSB and selling XRP without registering with FinCEN and by failing to implement and maintain an adequate AML program. Ripple Labs entered into a settlement agreement that resolved possible criminal charges and required the entity to forfeit \$450,000. These funds were credited to partially satisfy the \$700,000 civil money penalty. In addition, the settlement agreement required Ripple Labs to engage in steps to ensure future compliance with AML/CFT obligations.<sup>68</sup>





## 2. Office of Foreign Assets Control

**Regulatory authority.** Virtual assets move globally, and in some instances they move to entities or jurisdictions subject to economic sanctions administered by the U.S. Department of the Treasury. The Treasury Department's Office of Foreign Assets Control ("OFAC") administers and enforces economic and trade sanctions against targeted foreign countries and regimes; terrorist groups; international narcotics traffickers; those engaged in activities related to the proliferation of weapons of mass destruction; those engaged in malicious cyber activities; and other entities that present threats to the national security, foreign policy, or economy of the United States based on U.S. foreign policy and national security goals.<sup>69</sup>

As a general matter, U.S. persons and persons otherwise subject to OFAC jurisdiction—including firms that facilitate or engage in online commerce or process transactions using digital currency<sup>70</sup>—are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions (such as dealings with blocked persons or property) or in otherwise-prohibited trade or investment-related transactions.<sup>71</sup> Prohibited transactions generally also include those that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under

various sanctions authorities.<sup>72</sup> In addition, persons who provide financial, material, or technological support for or to a designated person or entity, or certain malicious activities, may themselves be designated by OFAC under the relevant sanctions authority, or be criminally or civilly liable for violations of the Trading With the Enemies Act, the International Emergency Economic Powers Act, and other statutes.<sup>73</sup>

### ***Interaction with the Department of Justice.***

On November 28, 2018, OFAC took its first virtual-asset-related action pursuant to the "cyber sanctions" authorized by Executive Order ("EO") 13694, as amended by EO 13757.<sup>74</sup> This action targeted two Iran based individuals who helped exchange bitcoin ransom payments into Iranian rial on behalf of malicious Iranian cyber actors involved with the SamSam ransomware scheme described above.<sup>75</sup> OFAC also identified two bitcoin addresses associated with these individuals that were connected to over 7,000 transactions worth millions of dollars.<sup>76</sup> By designating these malicious cyber actors, OFAC sought to "aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards," while also encouraging "virtual currency exchanges, peer-to-peer exchangers, and other providers of digital currency services [to] harden their networks against [such] illicit schemes."<sup>77</sup> As described above, in a related move, the Department of Justice brought criminal charges against the two Iran-based individuals related to the 34-month-long international computer hacking and extortion scheme involving the use of SamSam ransomware against numerous U.S. computer networks.<sup>78</sup>



In August 2019, OFAC designated three Chinese nationals, one Chinese drug trafficking organization, and one Chinese pharmaceutical company for their involvement with fentanyl manufacturing and trafficking pursuant to the Foreign Narcotics Kingpin Designation Act (“Kingpin Act”). OFAC identified cryptocurrency addresses associated with two drug traffickers to maximize disruption of their financial dealings.<sup>79</sup> OFAC closely coordinated these designations with the Department of Justice. Previously, in 2017, the Department of Justice indicted one of the Chinese nationals for his role as a manufacturer and distributor of fentanyl and other opiate substances.<sup>80</sup> And in August 2018, the Department of Justice charged two of the Chinese nationals with operating a conspiracy that manufactured and shipped deadly fentanyl analogues and 250 other drugs to at least 25 countries and 37 states.<sup>81</sup>

In September 2020, OFAC designated three Russian nationals for having acted or purported to act for or on behalf of, directly or indirectly, the Internet Research Agency (“IRA”), an entity previously designated for its involvement with election interference activities, pursuant to EO 13694, as amended by EO 13757, and EO 13848. The IRA uses cryptocurrency to fund activities in furtherance of ongoing malign influence operations around the world. OFAC identified digital currency addresses for two of these Russian nationals.<sup>82</sup> Concurrently, the Department of Justice filed a criminal complaint charging one of the Russian nationals for his alleged role in a conspiracy to use the stolen identities of real U.S. persons

to open fraudulent accounts at banking and cryptocurrency exchanges.<sup>83</sup>

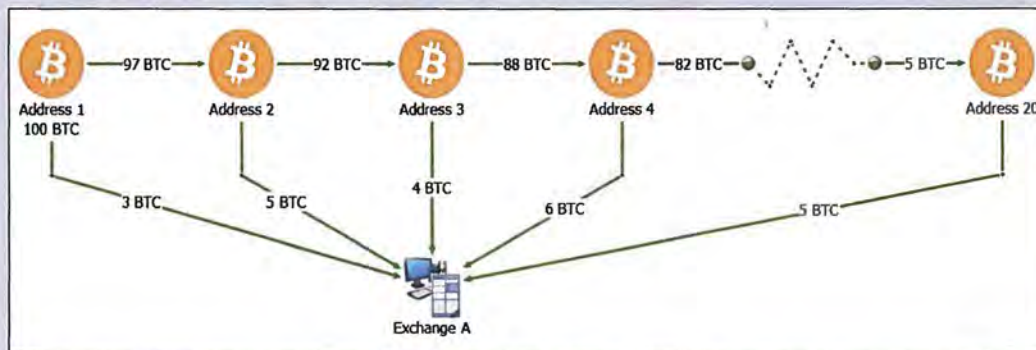
Earlier, on March 2, 2020, OFAC announced sanctions pursuant to EOs 13722 and 13694, as amended, against two Chinese nationals who are alleged to have laundered over \$100 million worth of cryptocurrency stolen from cryptocurrency exchanges by North Korean actors. This theft is another example of North Korea’s cyber heist program (see page 28), which trains actors to target and launder stolen funds—including large amounts of cryptocurrency—from financial institutions.<sup>84</sup> The two sanctioned individuals allegedly received the stolen cryptocurrency from accounts controlled by North Korean actors and subsequently transferred the funds among cryptocurrency addresses to obfuscate their origin. As a result of OFAC’s action, “all property and interests in property of these individuals that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC.”<sup>85</sup> On the same day that OFAC announced these sanctions, the Department of Justice announced criminal charges against the two individuals for money laundering conspiracy and for operating an unlicensed money transmitting business, as well as the seizure of the illicit funds.<sup>86</sup> Subsequently, on August 27, 2020, the Department filed a complaint seeking civil forfeiture of 280 additional virtual currency addresses and accounts linked to the hacks.<sup>87</sup> The coordinated actions by OFAC and the Department of Justice followed a comprehensive investigation led by the FBI, IRS–Criminal Investigation, and Homeland Security Investigations, further demonstrating the importance of cooperation among investigatory agencies.



### CASE STUDY: THE NORTH KOREAN HACKS

As discussed in the text, on the same day in March 2020 that OFAC announced sanctions, the Department of Justice announced criminal charges against two Chinese nationals for laundering over \$100 million worth of cryptocurrency that the defendants allegedly obtained from North Korean actors who had hacked cryptocurrency exchanges.<sup>88</sup> In March and August 2020, the Department also announced complaints seeing the civil forfeiture of hundreds of virtual currency accounts associated with related North Korean hacks and subsequent money laundering conspiracies.<sup>89</sup> The investigations into these criminal schemes revealed highly sophisticated money-laundering techniques. For example, criminal actors allegedly laundered the funds illicitly obtained from the hacks through several intermediary addresses and other virtual currency exchanges. On several occasions, the actors allegedly used the chain-hopping technique in an attempt to obfuscate the transaction path by converting the stolen cryptocurrency into BTC, Tether, or other forms of cryptocurrency.<sup>90</sup> The actors also allegedly used “peel chains” to conceal their activity, whereby “a large amount of [cryptocurrency] sitting at one address is sent through a series of transactions in which a slightly smaller amount of [cryptocurrency] is transferred to a new address each time.”<sup>91</sup>

**Figure 12: Depiction of a Simple “Peel Chain”**



*This chart depicts a hypothetical “peel chain” where a subject deposits 100 total bitcoin into an exchange. The subject forwards the bitcoin through a series of 20 “peels” in inconsistent amounts in an attempt to make the underlying transaction difficult to track. In practice, sophisticated cybercriminals often use hundreds of transactions to obscure the path of funds.<sup>92</sup>*

The successful investigations into the North Korean cryptocurrency hacks and subsequent money-laundering scheme—and the coordinated actions between OFAC and the Department of Justice—demonstrate the importance of interagency coordination in addressing threats within the virtual currency space.





### 3. Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency ("OCC") is an independent branch of the U.S. Department of the Treasury that charters, regulates, and supervises national banks and federal savings associations. OCC issues rules and regulations for banks and can "impos[e] corrective measures, when necessary, on OCC-governed banks that do not comply with laws and regulations or that otherwise engage in unsafe or unsound practices."<sup>93</sup> On July 22, 2020, OCC published an Interpretive Letter to clarify the authority of national banks and federal savings associations to provide cryptocurrency custody services for their customers.<sup>94</sup> The Letter concludes that such services, which include "holding the unique cryptographic keys associated with cryptocurrency," are a permissible modern form of traditional bank activities.<sup>95</sup> It also stressed OCC's position that banks can provide their services to lawful cryptocurrency businesses "so long as they effectively manage the risks and comply with applicable law."<sup>96</sup>

Earlier in 2020, OCC entered into a cease-and-desist consent order with M.Y. Safra Bank, after alleging that the bank violated the BSA's requirements for establishing an adequate AML program and failed to

investigate suspicious transactions and to timely file SARs. Among other things, OCC's investigation revealed that the bank failed to sufficiently consider AML risks and implement appropriate risk controls when opening accounts for customers that operated virtual-currency money services businesses.<sup>97</sup> Pursuant to the consent order, the bank must adopt numerous improvements to its risk profile, system of internal controls, customer due diligence operation, and BSA audit program.



### 4. The Securities and Exchange Commission

**Regulatory authority.** The mission of the U.S. Securities and Exchange Commission ("SEC") is to protect investors; to maintain fair, orderly, and efficient markets; and to facilitate capital formation. Of particular relevance to the SEC's mission in the virtual currency context is the rapid growth of the "initial coin offerings" ("ICOs") market and its widespread promotion as a means for new investment opportunity, which has provided fertile ground for malicious actors to swindle investors. ICOs (which are also known as "token sales"<sup>98</sup>) are a means companies have used to raise capital by offering and selling digital tokens to potential investors in exchange for funding a certain project or platform. The tokens purchased by an investor in an ICO, which are distributed



via a blockchain network, typically do not provide traditional “shares” in the issuing company. Instead, they might purport to grant access to a good or service, to the right to a share in the relevant project’s earnings, or to a potential increase in value based on the project’s success.<sup>99</sup> Recognizing the securities law implications for technological developments like blockchain and distributed ledger technologies, digital assets (including cryptocurrency), digital asset securities, and other digital instruments, the SEC has devoted substantial resources to this area.<sup>100</sup>

In 2017, the SEC issued an investigative report cautioning the public that offers and sales of digital assets—including through ICOs and token sales—by “virtual” organizations may be subject to the requirements of the federal securities laws, which include registration and disclosure mandates.<sup>101</sup> As the SEC explained, “[w]hether or not a particular transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction.”<sup>102</sup> To protect investors and the public, the SEC has summarily suspended, for 10 business days, the trading of securities of more than a dozen issuers when there were concerns about the accuracy and adequacy of information in the marketplace regarding securities offered or sold through ICOs or coin- or token- related news.<sup>103</sup> The SEC also has warned investors about potential scams involving companies claiming to be related to, or asserting they are engaging in, ICOs. And the SEC has filed ICO-related civil enforcement actions against individuals violating the securities laws or engaging in fraudulent schemes.<sup>104</sup>

On April 3, 2019, the SEC Staff released a framework for analyzing whether “a digital asset is offered or sold as an investment contract, and, therefore, is a security” under the federal securities laws.<sup>105</sup> The term “security” includes an “investment contract,” as well as other instruments such as stocks, bonds, and transferable shares. Under the so-called “*Howey* test,” derived from the Supreme Court’s seminal 1946 decision in *Securities and Exchange Commission v. W. J. Howey Co.*, an “investment contract” exists if there is an investment of money in a common enterprise with an expectation of profits derived from the efforts of others.<sup>106</sup> The framework is careful to note that, in the digital asset context, as with all other assets, this analysis does not depend only on the “form and terms” of the asset itself, “but also on the circumstances surrounding the digital asset and the manner in which it is offered, sold, or resold.”<sup>107</sup> The SEC encourages individuals and entities in the digital asset marketplace to engage proactively with SEC staff as the marketplace continues to develop.<sup>108</sup>

A high-profile action brought by the SEC in October 2019 highlights the need for individuals and entities in the global digital asset marketplace to ensure they are in compliance with U.S. federal securities laws. That month, the SEC sought and received a temporary restraining order against two offshore entities conducting an unregistered, ongoing digital token offering both within the United States and overseas that had raised more than \$1.7 billion of investor funds.<sup>109</sup> According to the SEC’s complaint, “Telegram Group Inc. and its wholly-owned subsidiary



TON Issuer Inc. began raising capital in January 2018 to finance the companies' business, including the development of their own blockchain, the 'Telegram Open Network' or 'TON Blockchain,' as well as the mobile messaging application Telegram Messenger.<sup>110</sup> As part of their plan to raise funds, the entities sold "approximately 2.9 billion digital tokens called 'Grams' at discounted prices to 171 initial purchasers worldwide, including more than 1 billion Grams to 39 U.S. purchasers."<sup>111</sup> The SEC's complaint alleged that Telegram and TON Issuer failed to register their offers and sales of the new "Grams" cryptocurrency, in violation of the registration provisions of the Securities Act of 1933.<sup>112</sup>

In March 2020, a federal judge granted the SEC a preliminary injunction, ruling that the agency had shown "a substantial likelihood of success in proving that the contracts and understandings at issue, including the sale of 2.9 billion Grams to 175 purchasers in exchange for \$1.7 billion, are part of a larger scheme to distribute those Grams into a secondary public market, which would be supported by Telegram's ongoing efforts."<sup>113</sup> Accordingly, the court concluded that, on the facts before it, "the resale of Grams into the secondary public market would be an integral part of the sale of securities without a required registration statement."<sup>114</sup> Three months later, the court approved a settlement between the parties, whereby Telegram and its subsidiary agreed not to appeal the court's ruling and consented to the court's judgment without admitting or denying the SEC's allegations. The court ordered Telegram to disgorge \$1,224,000,000 in ill-gotten gains

from the sale of Grams, with credit for the amounts paid back to initial purchasers of Grams, and also ordered Telegram to pay a civil penalty of \$18,500,000.<sup>115</sup>

The SEC's landmark Telegram case underscores why companies and individuals working and innovating in the digital assets space should ensure—prior to offering or selling—that their activities will meet all applicable requirements under the federal securities laws.<sup>116</sup> Of course, in cases involving outright fraud, bad actors face not only a variety of potential civil securities law violations, but also potential criminal prosecution for fraud or theft.<sup>117</sup>

***Interaction with the Department of Justice.*** The SEC works closely with the Department of Justice in cases involving criminal violations of the federal securities laws, including cases related to ICOs. As just one example, on January 25, 2018, the SEC filed a civil complaint in federal court in Texas seeking to halt an allegedly fraudulent ICO by AriseBank. The same week, the FBI and the SEC coordinated the timing of a search at the temporary residence of the ICO issuer with the execution of a freeze order by a receiver in the SEC's civil action, resulting in the recovery of cryptocurrency for the victim investors.<sup>118</sup> Subsequently, in the Department of Justice's related criminal case, a federal grand jury in Dallas charged AriseBank CEO Jared Rice, Sr., on November 20, 2018, for defrauding investors out of \$4 million worth of cryptocurrency assets. The Department's investigation revealed that Rice claimed in connection with the ICO that a cryptocurrency token called "AriseCoin"



could offer consumers FDIC insured accounts and traditional banking services, in addition to cryptocurrency services. These statements were false. Rice, who had converted investor funds for his own personal use, also claimed falsely that the ICO had raised \$600 million in a matter of weeks.<sup>119</sup> On March 20, 2019, Rice pleaded guilty in the criminal proceedings to one count of securities fraud, in violation of 15 U.S.C. §§ 78j and 78ff. In the SEC's civil action, Rice and AriseBank COO Stanley Ford agreed to pay nearly \$2.7 million in disgorgements, interest, and penalties, without admitting or denying the allegations. Both Rice and Ford are permanently enjoined from violating the antifraud and registration provisions of the federal securities laws, from ever serving as officers or directors of public companies, and from participating in issuances, offers, or sales of digital securities.<sup>120</sup>



## 5. The Commodity Futures Trading Commission

**Statutory authority.** Like the SEC, the Commodity Futures Trading Commission ("CFTC") has statutory authority with respect to certain aspects and uses of virtual assets. Under the Commodity Exchange Act ("CEA"),<sup>121</sup> the CFTC has oversight over derivatives contracts, including futures, options, and swaps,<sup>122</sup> that involve a

commodity. The CEA defines "commodity" to include agricultural products, "all other goods and articles," and "all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in."<sup>123</sup> The CFTC has concluded that certain virtual currencies are "commodities" under the CEA.<sup>124</sup> In addition, multiple federal courts have held that virtual currencies fall within the CEA's definition of commodity.<sup>125</sup>

The CFTC's jurisdiction is implicated when a virtual currency is the underlying asset in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce. "Beyond instances of fraud or manipulation, the CFTC generally does not oversee 'spot' or cash market exchanges and transactions involving virtual currencies which do not utilize margin, leverage, or financing."<sup>126</sup> The CFTC has taken action against unregistered bitcoin futures exchanges and firms illegally offering margined or financed retail virtual currency transactions;<sup>127</sup> enforced laws prohibiting fictitious trades on a derivatives platform<sup>128</sup> and laws requiring firms to implement adequate anti-money laundering procedures;<sup>129</sup> issued interpretative guidance concerning whether "actual delivery" has occurred in the context of retail commodity transactions in virtual currencies;<sup>130</sup> issued warnings about valuations and volatility in spot virtual currency markets;<sup>131</sup> and addressed numerous virtual currency Ponzi schemes.<sup>132</sup>

**Interaction with the Department of Justice.** In a case involving parallel action by the Department of Justice, the CFTC on April



16, 2018, filed a complaint in federal court in New York charging Blake Harrison Kantor and Nathan Mullins, as well as several entities located in the United States and abroad, with operating a fraudulent scheme covering binary options and a virtual currency known as ATM Coin.<sup>133</sup> The CFTC's complaint alleged that, since at least April 2014, the defendants solicited potential customers through emails, phone calls, and a website to purchase illegal off-exchange binary options. Additionally, the defendants falsely claimed that customers' accounts would generate significant profits based upon Kantor's purported profitable trading history, and allegedly misappropriated a substantial amount of the customer funds for personal use. The defendants were alleged to have sought to cover up their misappropriation by inviting customers to transfer their binary options account balances into ATM Coin. Some customers agreed to transfer their funds into ATM Coin, and at least one customer sent additional money to the defendants to purchase additional ATM Coin. The defendants then allegedly misrepresented to customers that their ATM Coin holdings were worth substantial sums of money. On October 23, 2019, a federal court entered an order finding that the defendants had committed fraud and had misappropriated client funds, and requiring them to pay a total of \$4.25 million.<sup>134</sup> In a parallel action, the United States Attorney for the Eastern District of New York filed a criminal indictment charging Kantor with fraud, obstruction, and making false statements. He pleaded guilty to the wire fraud conspiracy and obstruction charges, and was sentenced on July 1, 2019, to 86 months' imprisonment.<sup>135</sup>



## 6. The IRS and Tax Enforcement

The Internal Revenue Service ("IRS") treats virtual currency as property for U.S. federal tax purposes, which means that the general tax principles that apply to property transactions also apply to virtual currency transactions.<sup>136</sup> Income, including capital gains, from virtual currency transactions is taxable, and virtual currency transactions themselves must be reported on a taxpayer's income tax return.<sup>137</sup>

In addition, wages paid in virtual currency to employees are taxable, reportable on a Form W-2, and subject to withholding and payroll taxes. Businesses that receive payments for goods or services in virtual currency are required to include such payments in their gross income. The Department of Justice's Tax Division and U.S. Attorney's Offices around the country may pursue tax related prosecutions in cases involving the failure to report income from virtual currency. The Department of Justice also works with the IRS to support its enforcement and compliance efforts relating to virtual currency, including enforcing summonses issued to taxpayers and third parties, as well as assisting in "John Doe" summons matters.<sup>138</sup>



On October 9, 2019, the IRS issued additional guidance and FAQs for taxpayers who engage in virtual currency transactions, in an effort to help them better understand their reporting obligations. The guidance addresses the tax treatment of “hard forks,” which occur when a cryptocurrency undergoes a protocol change resulting in a new distributed ledger and a new cryptocurrency, in addition to the original distributed ledger.<sup>139</sup> The FAQs also address more basic questions about, for example, calculating gains or losses when selling or exchanging virtual currency for real currency or property; whether virtual currency paid by an employer for services constitutes taxable income; and maintaining records of transactions in virtual currency.<sup>140</sup> On December 31, 2019, the IRS issued additional FAQs for taxpayers relating to charitable donations in virtual currency.<sup>141</sup>

## 7. State Authorities

State attorneys general, securities regulators, and departments of financial services are responsible for protecting the investing public in their respective States by, for example, licensing securities firms and investment professionals (such as broker-dealers and investment advisers); registering certain securities offerings; reviewing financial offerings by companies; auditing sales practices and record keeping; promoting investor education; and enforcing State securities and banking laws.<sup>142</sup> Many State authorities are actively monitoring, supervising, or investigating virtual asset activities within their jurisdictions,

particularly those involving the issuance or sale of ICOs and other investment products.

For example, on May 21, 2018, the North American Securities Administrators Association (“NASAA”)<sup>143</sup> announced a coordinated series of enforcement actions by State and provincial securities regulators in the United States and Canada to crack down on fraudulent ICOs and cryptocurrency-related investment products, as well as on the fraudsters behind them. More than 40 jurisdictions throughout North America participated in “Operation Cryptosweep,” which resulted in nearly 70 inquiries and investigations and 35 pending or completed enforcement actions related to ICOs or cryptocurrencies.<sup>144</sup>

The State of New York has been one of the more proactive States seeking to regulate and gather information in the virtual asset and ICO space. New York State officials are conducting a Virtual Markets Integrity Initiative, which is a fact-finding inquiry into the policies and practices of platforms used by consumers to trade cryptocurrencies.<sup>145</sup> As part of that initiative, on April 17, 2018, the New York Attorney General’s Office sent letters to thirteen entities identified as “major virtual currency trading platforms” or “exchanges,” requesting disclosures about their operations, use of bots, conflicts of interest, outages, and other issues.<sup>146</sup> The letters also requested information on the covered entities’ operations, internal controls, and safeguards to protect customer assets as part of a broader effort to protect cryptocurrency investors and consumers.



### C. International Regulation

As discussed further below, the lack of consistent international regulation and enforcement of anti-money laundering and combating the financing of terrorism standards applicable to virtual asset entities represents a major challenge. There are, however, important organizations in the international regulatory space, especially the global standard-setter for AML/CFT standards—the Financial Action Task Force (“FATF”).<sup>147</sup>



**The Financial Action Task Force.** The FATF is an intergovernmental organization that was founded in 1989 on the initiative of the G7 by the ministers of its member jurisdictions.<sup>148</sup> Its objectives are to set standards and to promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, proliferation of weapons of mass destruction, and other related threats to the integrity of the international financial system. As a standard-setting and policy-making body, the FATF works to generate the technical understanding and necessary political will to bring about national legislative and regulatory reforms, which are intended to be harmonized across jurisdictions to the greatest extent possible.

The FATF reviews money laundering and terrorist financing techniques and countermeasures; provides a forum for exchange of best practices; highlights areas of common concern; and promotes and monitors the progress of its members in adopting and implementing regulatory measures globally. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities as part of its peer review process with the aim of protecting the international financial system from misuse, as well as creating standards for national best practices.

***The FATF Recommendations and Virtual Asset Guidance.*** The FATF has developed a series of “Recommendations” that are recognized as the international standards for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. FATF member countries are responsible for implementing the standards at the national level for compliance by the private sector. This provides the foundation for a coordinated international response aimed at confronting these threats to the integrity of the global financial system.

In 2014, the FATF recognized the need to bring virtual-asset-related activities within its scope, and in 2015 issued global guidance as part of a staged approach to addressing the money-laundering and terrorist-financing risks associated with virtual asset payment products and services. In July 2018, the FATF published a report at the G20 Finance Ministers and Central Bank Governors’ meeting outlining the FATF’s



commitment to addressing illicit finance threats involving virtual assets. Under the leadership of the United States, which held the FATF presidency at the time, the FATF in October 2018 updated its standards to clarify their application to virtual asset activities by amending “Recommendation 15” and adding two new glossary definitions—“virtual asset” and “virtual asset service provider.” Recommendation 15, which covers new technologies, states:

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.<sup>149</sup>

On June 21, 2019, the FATF adopted and issued a revised Interpretive Note to Recommendation 15 (“INR. 15”) that further clarifies and expands upon the FATF’s amendments to the standards relating to virtual assets, and describes how countries and obliged entities must comply with the relevant Recommendations to prevent the misuse of virtual assets for money laundering, terrorist financing, and proliferation.<sup>150</sup> Along with updated and expanded guidance aimed at assisting international jurisdictions and the private sector in implementing a risk-based approach to virtual assets and VASPs, INR. 15 requires countries to ensure that VASPs assess and mitigate their money laundering and terrorist financing risks, and implement

the full range of AML/CFT preventive measures under the Recommendations—just like other entities subject to AML/CFT regulation. These measures include customer due diligence, record keeping, suspicious transaction reporting, and screening of transactions for compliance with targeted financial sanctions, among others.<sup>151</sup>

***Interaction with the Department of Justice.***

The United States is a founding member of the FATF and, while holding the FATF presidency from July 2018 through June 2019, made it a priority to regulate VASPs for AML/CFT. The U.S. delegation to the FATF is led by the Department of the Treasury’s Office of Terrorist Financing and Financial Crimes, and includes the Department of Justice as a key interagency partner. The delegation urged that all FATF Recommendations broadly apply to VASPs and virtual asset financial activities, which resulted in the successful adoption of the amendments to Recommendation 15 along with the Interpretive Note and guidance discussed above. Department of Justice attorneys provided significant contributions to the drafting and adoption process for these important changes to the FATF standards. The FATF also pursues ongoing work on trends in AML/CFT risk related to virtual assets, such as publicly identifying red flags in virtual asset financial activity, and issuing reports that provide case studies drawn from all over the FATF’s global network. The Department of Justice has been an integral partner in this effort, providing analysis and case examples for the U.S. delegation.



### III. Ongoing Challenges and Future Strategies

Parts I and II of this Framework discussed some of the serious public safety challenges posed by the misuse of cryptocurrency, and the legal and regulatory authorities the Department of Justice and its partners have used to address those challenges. This final Part explores the obligations of certain business and other entities that are particularly susceptible to abuse in the cryptocurrency space, and describes the Department's ongoing strategies for addressing these emerging threats to the safe and effective operation of the cryptocurrency marketplace.

#### A. Business Models and Activities That May Facilitate Criminal Activity

As described above, certain MSBs and other types of VASPs play a key role in the cryptocurrency ecosystem. Given their potential to facilitate criminal activity, these entities have a heightened responsibility to safeguard their platforms and businesses from exploitation by nefarious actors and to ensure that customer data is protected and secured. Moreover, the proper collection and maintenance of customer and transactional information by MSBs and other financial institutions pursuant to the BSA is crucial to the Department's ability to identify illicit actors, investigate criminal activity, and obtain evidence necessary for prosecutions. Key industry participants bearing these responsibilities include not only conventional virtual asset exchanges and brokers, but also peer-to-peer exchangers, kiosk operators,

and online casinos, as discussed further below. Unfortunately, many entities in these new and growing sectors often fail to comply, in whole or in part, with the BSA and other legal requirements, thereby threatening the Department's investigative abilities and undermining public safety.

**Cryptocurrency exchanges.** Companies and individuals that offer cryptocurrency and other virtual asset exchange services to the public are commonly referred to as "exchanges" and "exchangers." Even exchanges that do not accept fiat currency and operate only with cryptocurrency are obliged to follow FinCEN record keeping and reporting requirements, as the applicable regulations cover transfers of value and are not specific to fiat transactions. Moreover, all entities, including foreign-located exchanges, that do business wholly or in substantial part within the United States, such as by servicing U.S. customers, must also register with FinCEN and have an agent physically present in the United States for BSA reporting and for accepting service of process.<sup>152</sup>

**Peer-to-peer exchangers and platforms.** Individuals seeking to buy or sell cryptocurrency other than through registered or licensed exchanges and financial institutions frequently turn to networks of individuals commonly referred to as peer-to-peer ("P2P") exchangers or traders. As individuals who facilitate transfers of value for the public, including the buying and selling of cryptocurrency, P2P exchangers are considered MSBs and are subject to FinCEN record keeping and reporting requirements.<sup>153</sup> In practice, however, many



## Cryptocurrency Exchanges

- Allow users to buy and sell cryptocurrencies
- Serve as a conduit to the traditional financial system
- Can convert cryptocurrency to other virtual currencies or to fiat currency
- Global entities that can move money in seconds, not days
- In the U.S., exchanges are regulated by FinCEN as money service businesses
- In the international space, exchanges are subject to inconsistent regulatory regimes

P2P exchangers fail to register with FinCEN as MSBs or to comply with BSA obligations, and some even conduct transactions without requiring any form of identification from the customer.

P2P exchangers usually charge substantially higher percentage rates or fees—or use less favorable exchange rates—than registered exchanges. They often will accept a wide variety of payment methods, including payments of fiat currency in person or through the mail, deposits into bank accounts, Western Union or MoneyGram transfers, or payments in gift cards or stored value cards. P2P exchangers generally find their customers through word of mouth, open source websites such as Craigslist, or online exchange platforms.

P2P exchangers commonly use online exchange platforms or websites that allow users to trade virtual assets directly with one another and without a central operator. Nonetheless, when engaging in the transmission of virtual assets, these platforms must comply with BSA requirements. Although many P2P exchange platforms offer services similar to those offered by centralized

virtual asset exchanges, P2P exchange platforms provide opportunities for cross-platform trading of cryptocurrency without the use of traditional financial institutions. Furthermore, unlike centralized virtual asset exchanges, P2P exchange platforms may operate without an intermediary that will accept and transmit virtual assets in exchange for fiat or another type of virtual asset, or that will collect customer identification information. Individual exchangers—as well as platforms and websites—that fail to collect and maintain customer or transactional data or maintain an effective AML/CFT program may be subject to civil and criminal penalties.<sup>154</sup>

**Cryptocurrency kiosks.** Cryptocurrency kiosks, which are commonly referred to as “Bitcoin ATMs,” are stand-alone machines that allow users to convert fiat currency to and from bitcoin and other cryptocurrencies. With these machines, cryptocurrency can be bought or sold directly using a customer’s mobile device or delivered in the form of a paper wallet. Thus, cryptocurrency kiosks offer an easy-to-use physical access point for virtual asset exchange.



### Cryptocurrency Kiosks (aka Bitcoin ATMs)

- ATM-like machines that facilitate the buying, selling, and/or exchange of bitcoin or other cryptocurrencies
- Can be located almost anywhere, including malls, convenience stores, gas stations, and grocery stores
- Often charge much higher transaction fees for services than other types of cryptocurrency exchanges
- Capture different types of identifying information, including photographs or video
- Kiosk operators are considered money service businesses and are subject to anti-money laundering regulations and other legal requirements



Cryptocurrency kiosk operators are considered MSBs in the United States. Accordingly, they are subject to the BSA and must register with FinCEN and follow all applicable money transmission requirements, including collecting and maintaining KYC data on their clients,<sup>155</sup> reporting suspicious transactions to FinCEN, filing currency transaction reports for fiat transactions of \$10,000 or more in cash, and maintaining an effective AML/CFT program. While some operators comply with these requirements, many kiosks are not BSA-compliant and fail to collect required customer and transaction

information. Indeed, investigators have linked such kiosks to illicit use by drug dealers, credit card fraud schemers, prostitution rings, and unlicensed virtual asset exchangers.

**Virtual currency casinos.** The rising popularity of virtual assets has led to the growth of virtual-currency-based “casinos” that facilitate various forms of betting denominated in bitcoin and other virtual currencies. Under current law, a casino that has gross annual gaming revenue in excess of \$1 million must be duly licensed



## HEROCOIN

On July 22, 2020, the Department of Justice announced that a California man agreed to plead guilty to operating an illegal virtual-currency money services business called Herocoin that exchanged up to \$25 million—including proceeds of criminal activity—through in-person transactions and a network of Bitcoin ATM-type kiosks. The kiosks were installed in malls, gas stations, and convenience stores throughout California, and allowed customers to exchange cash for bitcoin and vice versa. In his plea agreement, the defendant admitted that he intentionally failed to register Herocoin with FinCEN, and failed to implement an effective anti-money laundering program; file currency transaction reports for exchanges in excess of \$10,000; conduct due diligence on customers; or file suspicious activity reports. With respect to the Bitcoin ATM network, the defendant also admitted that he failed to implement a program to obtain identifications for customers conducting multiple transactions of up to \$3,000 or verify that any identification provided actually reflected the person conducting the transaction. After pleading guilty, the defendant will face a statutory maximum sentence of 30 years in federal prison, and will forfeit cash, cryptocurrency, and 17 Bitcoin ATMs.<sup>156</sup>

**Figure 13: Image of Cryptocurrency Kiosks Seized in the Herocoin Case**





or authorized to do business as a casino in the United States by a federal, State, or tribal authority.<sup>157</sup> Casinos that do not meet this criterion are considered MSBs. Whether regulated as casinos or MSBs, these gambling businesses are subject to the BSA and its KYC record keeping and reporting requirements. Traditional brick-and-mortar casinos generally do not accept bitcoin or other cryptocurrencies; however, online gambling sites increasingly do accept cryptocurrencies. Online casinos that provide gambling services are also MSBs and must comply with applicable money transmission regulations. Although many do not have a known physical location, they still are required to report suspicious transactions to FinCEN if they offer services to U.S. customers.

***Anonymity enhanced cryptocurrencies.***

The acceptance of anonymity enhanced cryptocurrencies or “AECs”—such as Monero, Dash, and Zcash—by MSBs and darknet marketplaces has increased the use of this type of virtual currency. As discussed above, because AECs use non-public or private blockchains, use of these cryptocurrencies may undermine the AML/CFT controls used to detect suspicious activity by MSBs and other financial institutions, and may limit or even negate a business’s ability to conduct AML/CFT checks on customer activity and to satisfy BSA requirements. Some AECs, however, offer features, such as public view keys, that potentially can facilitate the fulfillment of AML/CFT obligations, depending upon the implementation of such features.

The Department considers the use of AECs to be a high-risk activity that is indicative

of possible criminal conduct. In most circumstances, the Department does not liquidate seized or forfeited AECs, as doing so allows them to re-enter the stream of commerce for potential future criminal use. Companies that choose to offer AEC products should consider the increased risks of money laundering and financing of criminal activity, and should evaluate whether it is possible to adopt appropriate AML/CFT measures to address such risks.

AECs are often exchanged for other virtual assets like bitcoin, which may indicate a cross-virtual-asset layering technique for users attempting to conceal criminal behavior. This practice, which is commonly referred to as “chain hopping,” is discussed further below.

***Mixers, tumblers, and chain hopping.***

“Mixers” and “tumblers” are entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination. For a fee, a customer can send cryptocurrency to a specific address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers before sending it to the requested recipient address. Websites or companies offering mixing or tumbling services are engaged in money transmission, and therefore are MSBs subject to the BSA and other similar international regulations. In addition to facing BSA liability for failing to register, conduct AML procedures, or collect customer identification, operators of these services can be criminally liable for money laundering because these mixers and tumblers are designed specifically to

Figure 14: Example of a Criminal “Mixing” Enterprise

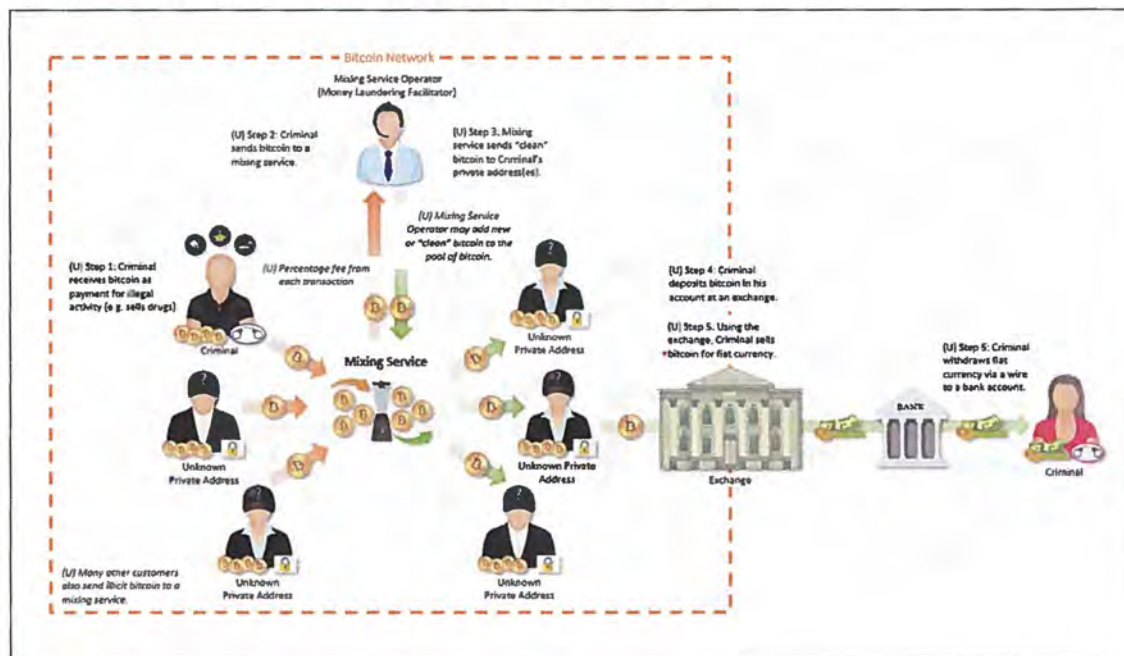
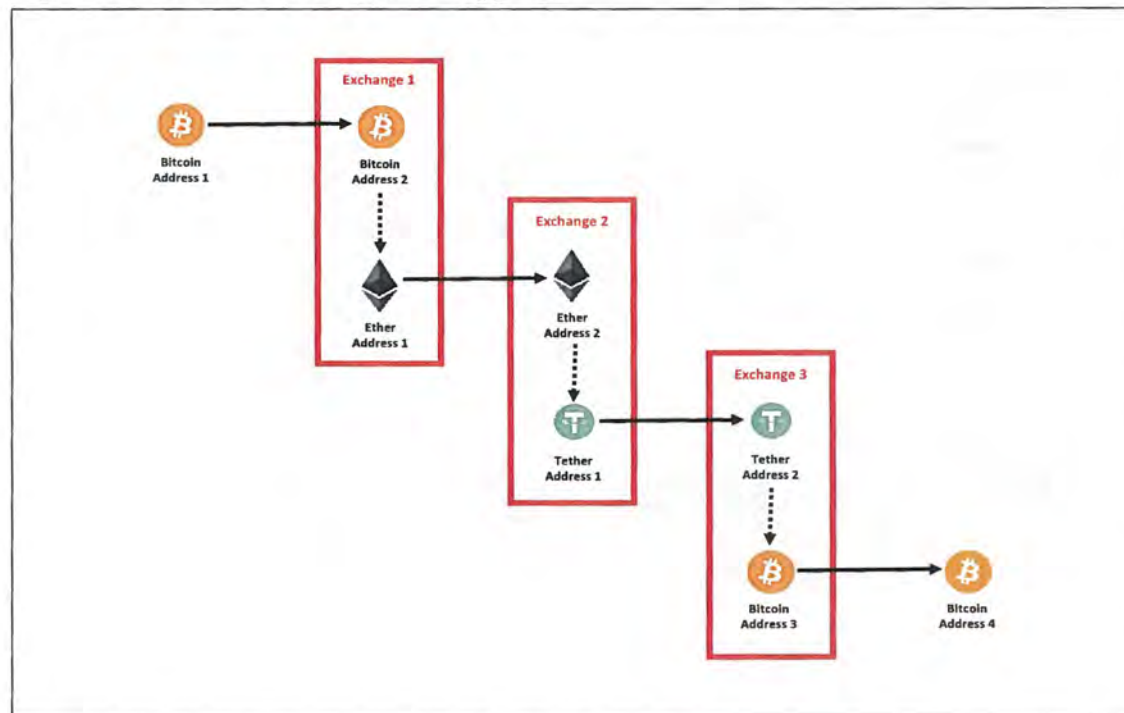


Figure 15: Illustration of “Chain Hopping”



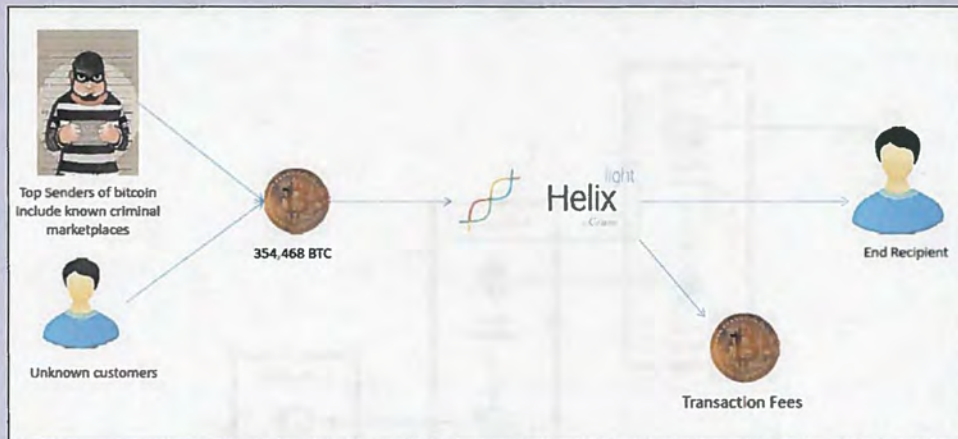


## HELIX

On February 13, 2020, the Department of Justice announced the indictment and arrest of the alleged administrator of Helix, a darknet cryptocurrency laundering service. According to the indictment, Helix functioned as a bitcoin “mixer” or “tumbler,” allowing customers to send bitcoin to designated recipients in a manner that was designed to conceal their source or owner.

The service’s administrator is alleged to have advertised Helix to customers on the darknet as a way to conceal transactions from law enforcement. The indictment charges Helix with laundering over \$300 million of bitcoin, which allegedly represented the proceeds of illicit narcotics sales and other criminal transactions.<sup>158</sup>

**Figure 16: Helix Allegedly “Tumbled” a Large Volume of Bitcoin, Charging a Fee for Each Transaction**



*Helix allegedly received more than 354,468 bitcoin between the site’s launch in June 2014 and December 2017, valued at approximately \$311 million in U.S. dollars at the time of the transactions.*



“conceal or disguise the nature, the location, the source, the ownership, or the control” of a financial transaction.<sup>159</sup>

Criminals also may engage in a practice known as “chain hopping,” in which they move from one cryptocurrency to another, often in rapid succession. As the Department has observed, chain hopping is “frequently used by individuals who are laundering proceeds of virtual currency thefts.”<sup>160</sup> Chain hopping is often viewed as a potential way to obfuscate the trail of virtual currency by shifting the trail of transactions from the blockchain of one virtual currency to the blockchain of another virtual currency.

***Jurisdictional arbitrage and compliance deficiencies.*** Because of the global and cross-border nature of transactions involving virtual assets, the lack of consistent AML/CFT regulation and supervision over VASPs across jurisdictions—and the complete absence of such regulation and supervision in certain parts of the world—is detrimental to the safety and stability of the international financial system.<sup>161</sup> This inconsistency also impedes law enforcement’s ability to investigate, prosecute, and prevent criminal activity involving or facilitated by virtual assets. For example, illicit financial flows denominated in virtual assets may move to companies and exchanges in jurisdictions where authorities lack regulatory frameworks requiring the generation and retention of records necessary to support investigations.

In the United States, AML/CFT standards have been in place for MSBs engaged in virtual asset activities since 2011, and yet many VASPs still are operating in ways

that do not comply with the BSA and other regulatory requirements. For example, some VASPs apply different standards to U.S. customers versus customers in other countries, while other VASPs actively apply different standards to virtual-asset-to-fiat transactions than to virtual-asset-to-virtual-asset transactions. Such behaviors are flatly inconsistent with VASPs’ BSA obligations and can create significant financial intelligence gaps.

## **B. Department of Justice Response Strategies**

***Investigations and prosecutions generally.*** Consistent with its mission to protect public safety and national security, the Department of Justice will continue its aggressive investigation and prosecution of a wide range of malicious actors, including those who use cryptocurrencies to commit, facilitate, or conceal their crimes. For instance, the Department has prosecuted a number of individuals operating as P2P exchangers for money laundering and for violating the BSA.<sup>162</sup> Many of these exchangers were selling virtual assets that they obtained from their own involvement in other criminal activities, such as drug trafficking or computer hacking, or were otherwise knowingly facilitating the criminal activities of others.

As discussed above, the Department has a broad range of legal authorities for investigating and prosecuting individuals who misuse cryptocurrency for criminal purposes. To that end, the Department is committed to an appropriate all-tools approach to dealing with cryptocurrency-related crime. The Department will continue



to engage actively with its regulatory partners to address the misuse and abuse of cryptocurrency by malicious actors. The case examples noted throughout this Framework highlight the many successes from the Department's work with regulatory partners such as FinCEN, OFAC, the SEC, the CFTC, and the IRS. By appropriately coordinating parallel enforcement actions, the Department can maximize its impact in investigating, dismantling, and deterring criminal activity; more effectively recover funds for victims; and better safeguard the financial system and the American public.

The Department also has robust authority to prosecute VASPs and other entities and individuals that violate U.S. law even when they are not located inside the United States. Where virtual asset transactions touch financial, data storage, or other computer systems within the United States, the Department generally has jurisdiction to prosecute the actors who direct or conduct those transactions. The Department also has jurisdiction to prosecute foreign-located actors who use virtual assets to import illegal products or contraband into the United States, or use U.S.-located VASPs or financial institutions for money laundering purposes. In addition, the Department may prosecute for violations of U.S. law those foreign-located actors who provide illicit services to defraud or steal from U.S. residents. Moreover, as FinCEN has observed, the BSA applies to entities and individuals that engage in money transmission as a business and that operate wholly or substantially in part in the United States, regardless of where they are incorporated or headquartered.

Finally, it bears emphasizing that if conduct involving virtual currency were to violate the U.S. statutes regarding material support of terrorism, the U.S. government could appropriately assert jurisdiction over such offenses anywhere in the world, consistent with due process, under the principle of protective jurisdiction. That principle holds that "[f]or non-citizens acting entirely abroad, a jurisdictional nexus exists when the aim of that activity is to cause harm inside the United States or to U.S. citizens or interests."<sup>163</sup> Where a malign actor's conduct involving cryptocurrency amounts to providing material support to a designated foreign terrorist organization, that actor engages in conduct that threatens the security of the United States, and therefore subjects himself (or itself) to the jurisdiction of our Nation's courts—and to the Department's enforcement of the Nation's laws.<sup>164</sup>

**Promoting law enforcement awareness and expertise.** Given the complexity of cryptocurrency technology and of the platforms on which it is used, law enforcement professionals across agencies must continually develop and maintain the base of knowledge and skills necessary to identify threats involving cryptocurrency; conduct robust and efficient investigations of those threats; and employ the many appropriate legal tools available to bring individuals and entities that abuse cryptocurrency to justice. The Department is taking the lead in this area by dedicating resources to existing initiatives and groups that encourage law enforcement awareness and expertise in the cryptocurrency space. These efforts include continuing to promote Department-wide,



### CASE STUDY: BTC-e

The BTC-e case, which was introduced earlier,<sup>165</sup> is one example of the Department of Justice's resolve to prosecute foreign-located entities and individuals in the cryptocurrency context. BTC-e operated globally as an unlicensed virtual currency exchange to launder and liquidate criminal proceeds from virtual currency to fiat currency. In doing so, it relied on the use of shell companies and affiliated entities that were similarly unregistered with FinCEN. According to its now-defunct website, BTC-e purported to be based in Eastern Europe. BTC-e's managing shell company, Canton Business Corporation, was registered in the Seychelles, and its web domains were registered to shell companies in, among other places, Singapore, the British Virgin Islands, France, and New Zealand. After a multi-year, multi-agency investigation, the Department successfully charged BTC-e and one of its principal operators with operating an unlicensed money services business, money laundering, and other related crimes.



Figure 17: BTC-e Website after Seizure by the U.S. Government



## CASE STUDY: ALPHABAY

The AlphaBay case, which also was mentioned previously,<sup>166</sup> further demonstrates the global reach of the Department of Justice, U.S. law enforcement, and our domestic and international partners in identifying and neutralizing unlawful activities involving cryptocurrency. At the time of its takedown by law enforcement in July 2017, AlphaBay was the dark web's largest criminal marketplace, serving over 200,000 users as a conduit for everything from illegal drugs and firearms to malware and toxic chemicals. Aided by the use of cryptocurrencies like Bitcoin, Monero, and Ether, AlphaBay's operators were able to hide the location and identities of the site's administrators and users and to facilitate the laundering of hundreds of millions of dollars. Over the course of the government's investigation, law enforcement identified AlphaBay proceeds and discovered hundreds of thousands of cryptocurrency addresses associated with the site.<sup>167</sup> The international operation to dismantle AlphaBay was led by the United States and involved cooperation from law enforcement partners in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, as well as the European law enforcement agency Europol.<sup>168</sup> The legal proceedings in the United States demonstrated the breadth of authorities the Department can and will bring to bear in appropriate cases.<sup>169</sup>

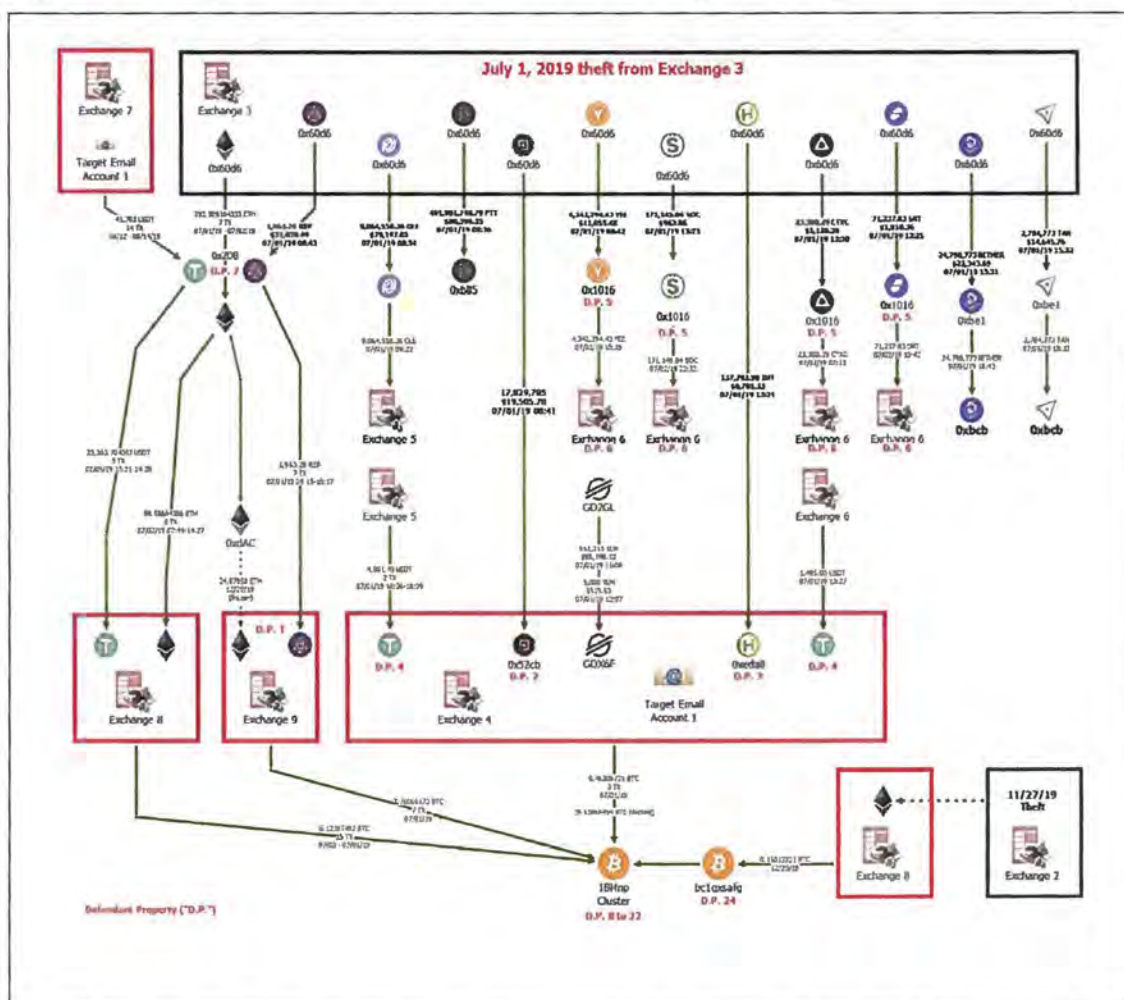


formalized training of investigators and prosecutors on the cryptocurrency threat and how best to address it; working with federal, State, local, and international partners to promote and coordinate the sharing of information and resources; serving as the main point of contact in cross-jurisdictional investigations; and conducting outreach to

the private sector in support of public-private partnerships.

The Department also will work with law enforcement agencies to develop further strategic guidance on the use of available legal tools to investigate and prosecute cryptocurrency-related offenses, and

**Figure 18: Example of an Illicit Transaction Path Developed Through Blockchain Analysis<sup>170</sup>**



This chart depicts a complex series of transactions following a theft from a virtual currency exchange ("Exchange 3"), including numerous conversions of cryptocurrency and deposits and withdrawals involving several intermediary addresses and exchanges. Successful investigations of such schemes require enhanced training and technical capabilities.



### THE DIGITAL CURRENCY INITIATIVE

As announced in the July 2018 Report of the Attorney General's Cyber Digital Task Force, the Money Laundering and Asset Recovery Section ("MLARS") within the Department of Justice's Criminal Division has established a Digital Currency Initiative to focus on "providing support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency prosecutions and forfeitures."<sup>171</sup> The Digital Currency Initiative continues to "expand and implement cryptocurrency-related training to encourage and enable more investigators, prosecutors, and Department components to pursue such cases, while developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture."<sup>172</sup>

consider legislative proposals to close any existing gaps in enforcement authority.

**Fostering cooperation with State authorities.** As discussed above, State attorneys general offices and regulatory agencies play an important role in protecting the investing public by enforcing State securities laws and licensing, registration, and auditing requirements. Coordination and de-confliction with State attorneys general offices, regulators, and prosecuting entities is crucial, and yet communication on matters involving virtual assets between federal prosecutors and State authorities currently varies by jurisdiction. United States Attorneys' Offices and Department litigating divisions should continue to develop lines of communication with State authorities handling securities and fraud investigations, prosecutions, and enforcement actions involving cryptocurrency and virtual-asset-related investment products. In addition, Department agencies should communicate and coordinate with State financial and banking authorities that regulate money transmitters operating in their respective

jurisdictions to prevent conflicts and duplication of efforts in money laundering prosecutions.

**Enhancing international cooperation and promoting comprehensive and consistent international regulation.** The inherently global nature of the virtual asset ecosystem poses significant investigative challenges for U.S. law enforcement agencies and for Department prosecutors. Effectively countering criminal activity involving virtual assets requires close international partnerships. Foreign partners assist U.S. law enforcement in, for example, conducting investigations, making arrests, and seizing criminal assets. Similarly, foreign partners may rely on the assistance of U.S. law enforcement to take action against individuals who commit crimes abroad and conceal evidence and assets—or themselves—within the United States. The Department will continue to encourage these partnerships in support of multi-jurisdictional parallel investigations and prosecutions, particularly those involving foreign-located actors, VASPs, and transnational criminal organizations.



## THE GDPR

In May 2018, the European Union (“EU”) General Data Protection Regulation 2016/679 (“GDPR”) came into effect. GDPR is a sweeping data protection and privacy law that applies to all data controllers, data processors, and data subjects within the EU’s jurisdiction. Some virtual currency exchanges have attempted to withhold data requested by law enforcement agencies in the United States through criminal grand jury subpoenas by citing GDPR’s broad privacy rules.

However, GDPR does not in fact bar companies subject to U.S. jurisdiction from complying with lawful requests in criminal investigations. To the contrary, GDPR explicitly permits the disclosure of data in a number of scenarios. For example, a virtual exchange that is subject to GDPR may process the requested data under GDPR Article 6(1) when “necessary for compliance with a legal obligation to which the controller is subject” or “necessary for the purposes of the legitimate interests pursued by the controller or by a third party . . . .”<sup>173</sup> Similarly, under Article 49.1, international transfer of data is permitted in various circumstances, including where “the transfer is necessary for important reasons of public interest” or “necessary for the purposes of compelling legitimate interests pursued by the controller.”<sup>174</sup>

The ability of law enforcement to investigate criminal activity is plainly an important reason of public interest, placing production of records pursuant to U.S. grand jury subpoenas squarely within the “public interest” exception in Article 49.1. Moreover, the transfer of data from exchanges may constitute a “compelling legitimate interest” in that the transfer may be necessary to prevent or defend against being held in contempt of court for failure to respond to lawful process. Indeed, the European Commission itself recognized this framework in a 2017 amicus brief it filed in the U.S. Supreme Court in *United States v. Microsoft*,<sup>175</sup> which discussed the GDPR’s rules governing the transfer of personal data to a non-EU state. In its brief, the European Commission recognized that the public interest is served by transferring data to non-EU countries to further international criminal investigations, stating: “[I]n general, [European] Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest.”<sup>176</sup>

GDPR Articles 6 and 49.1 provide additional legal bases for processing and transfer that may be applicable in particular circumstances. For example, Article 49.1(e) establishes a derogation if “the transfer is necessary for the establishment, exercise or [defense] of legal claims.”<sup>177</sup> This derogation may be applicable where the transfer of data from exchanges is sought pursuant to a subpoena or other compulsory order.

While the Department disagrees with the basis for such objections to lawful requests for information, some exchanges continue to cite to the GDPR while refusing to comply with standard grand jury subpoenas. The Department will continue to engage with these virtual currency exchanges to ensure compliance with lawful requests and will pursue motions to compel as needed.



The Department also works with its partners in the federal government to encourage their international counterparts to continue development of comprehensive and consistent international regulation of virtual assets. As discussed above, the Financial Action Task Force has adopted amendments to its Recommendation 15 that bring VASPs and virtual asset activity within the FATF's standards for AML/CFT. As implementation of these amendments expands across global jurisdictions, the Department will continue to provide policy support and subject matter expertise to the Department of the Treasury-led U.S. delegation, and to work internationally to level the legal and regulatory playing field related to virtual assets. In addition, other international organizations, including the United Nations Office on Drugs and Crime, are in the process of adopting regulatory frameworks that mirror the FATF's developing approach to virtual asset activity. We will monitor and actively contribute to those efforts, as appropriate.

Finally, the Department will continue to encourage its partners to support the adoption of consistent regulations across jurisdictions to prevent illicit actors from practicing jurisdictional arbitrage, and to ensure the collection of important evidence and seizure of illicit assets regardless of where an entity or illicit actor may be operating.

***Conducting private sector education and outreach.*** As with any specialized, technology-driven industry, effective regulation and policing of cryptocurrency activity requires close cooperation between the public and private sectors whenever

possible. This approach includes direct engagement with the companies that operate in the virtual asset space; with the banks and financial institutions that may be affected by virtual asset regulation; and, importantly, with the actual community of cryptocurrency users. In conducting such outreach, the Department and its partners will continue their efforts to advance mutual goals such as safeguarding the virtual asset marketplace from theft, fraud, and hacking.

## **Conclusion**

As the use of cryptocurrency evolves and expands, so too will opportunities to commit crime and to do harm by exploiting cryptocurrency technology. Every day, criminals expand and perfect techniques designed to evade detection and apprehension. Ultimately, illicit uses of cryptocurrency threaten not just public safety, but national security, as well. For example, cryptocurrency can provide terrorist organizations a tool to circumvent traditional financial institutions in order to obtain, transfer, and use funds to advance their missions. Current terrorist use of cryptocurrency may represent the first raindrops of an oncoming storm of expanded use that could challenge the ability of the United States and its allies to disrupt financial resources that would enable terrorist organizations to more successfully execute their deadly missions or to expand their influence.

Likewise, cryptocurrency presents a troubling new opportunity for individuals and rogue states to avoid international sanctions and to undermine traditional financial markets,

thereby harming the interests of the United States and its allies.

Despite the many challenges, the Department of Justice has aggressively investigated and prosecuted a range of malign actors who have used cryptocurrencies to facilitate or to conceal their illicit activities. Similarly, the Department has brought actions against individuals and companies that have failed to meet their legal obligations to counter illicit activity. In particular cases, we have even proceeded against the illicit cryptocurrency itself, seizing those virtual assets and removing them from the stream of international commerce, irrespective of our ability to identify or to apprehend the actors who used them. This essential work will continue, as the Department seeks to ensure that uses of cryptocurrency adhere to the law and are compatible with the protection of public safety and national security.

The Department of Justice, however, cannot achieve success on its own. We recognize the importance of working with interagency and

international partners to enhance an already vigorous enforcement plan, regulatory scheme, and policy framework to thwart the opportunities created by cryptocurrency for criminals, terrorists, and other bad actors. The Department is committed to strengthening its key partnerships by promoting law enforcement awareness and expertise; by fostering cooperation with State authorities; by enhancing international cooperation; by promoting comprehensive, consistent international regulation; and by conducting private sector education and outreach.

To promote public safety and protect national security, all stakeholders—from private industry to regulators, elected officials, and individual cryptocurrency users—will need to take steps to ensure cryptocurrency is not used as a platform for illegality. Indeed, for cryptocurrency to realize its truly transformative potential, it is imperative that these risks be addressed.









## NOTES

### Introduction

<sup>i</sup> The original formulation of this phrase (describing the laws as “those wise restraints that make men free”) was coined by Professor John MacArthur Maguire of Harvard. See <https://asklib.law.harvard.edu/faq/115309> (last accessed Oct. 1, 2020).

<sup>ii</sup> Jeff Sessions, Attorney General, “Memorandum for Heads of Department Components [Establishing Cyber-Digital Task Force],” Feb. 16, 2018, available at: <https://www.justice.gov/opa/press-release/file/1035457/download> (last accessed Oct. 1, 2020).

<sup>iii</sup> U.S. DEP’T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL’S CYBER-DIGITAL TASK FORCE 126 (2018), available at: <https://www.justice.gov/cyberreport> (last accessed Oct. 1, 2020).

<sup>iv</sup> U.S. DEP’T OF COMMERCE, NAT’L INST. OF STANDARDS AND TECH., “Blockchain,” available at: <https://www.nist.gov/topics/blockchain> (last accessed Oct. 1, 2020).

<sup>v</sup> U.S. DEP’T OF DEF, “DoD Digital Modernization Strategy,” at 44 (Appendix I), July 12, 2019, available at: <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF> (last accessed Oct. 1, 2020).

<sup>vi</sup> See U.S. FOOD AND DRUG ADMIN., “New Era of Smarter Food Safety: FDA’s Blueprint for the Future,” July 2020, available at: <https://www.fda.gov/media/139868/download> (last accessed Oct. 1, 2020).

<sup>vii</sup> Lael Brainard, Fed. Reserve Governor, “An Update on Digital Currencies,” Aug. 13, 2020, available at: <https://www.federalreserve.gov/newsevents/speech/brainard20200813a.htm> (last accessed Oct. 1, 2020).

<sup>viii</sup> BINANCE, “The Evolution of the Internet – Web 3.0 Explained,” Feb. 2020, available at: <https://academy.binance.com/en/articles/the-evolution-of-the-internet-web-3-0-explained> (last accessed Oct. 1, 2020).

### Cryptocurrency: An Enforcement Framework

<sup>1</sup> CTRS. FOR DISEASE CONTROL & PREVENTION, *Drug Overdose Deaths*, <https://www.cdc.gov/drugoverdose/data/statedeaths.html> (last accessed Oct. 1, 2020).

<sup>2</sup> FINANCIAL ACTION TASK FORCE (FATF), THE FATF RECOMMENDATIONS: INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 126 (June 2019) [hereinafter FATF INTERNATIONAL STANDARDS], available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (last accessed Oct. 1, 2020).

<sup>3</sup> Some countries, including the United States (see text accompanying *supra* note vii), are exploring the use of blockchain technology to support a national currency. Such currencies are sometimes referred to as “Central Bank Digital Currencies” or “CBDCs.” See, e.g., PRICEWATERHOUSECOOPERS, THE RISE OF CENTRAL BANK DIGITAL CURRENCIES (CBDCs) 2 (Nov. 2019), available at: <https://www.pwc.com/gx/en/financial-services/pdf/the-rise-of-central-bank-digital-currencies.pdf> (last accessed Oct. 1, 2020).



<sup>4</sup> U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FINCEN GUIDANCE FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (Mar. 18, 2013), available at: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (last accessed Oct. 1, 2020). A non-convertible virtual currency may effectively become a convertible virtual currency where a robust unofficial secondary market for the currency develops and provides the opportunity to exchange the "non-convertible" currency for fiat or other virtual currency. See FINANCIAL ACTION TASK FORCE (FATF), VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 4-5 (June 2014), available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (last accessed Oct. 1, 2020).

<sup>5</sup> Throughout this publication, specific examples of cryptocurrency, like Bitcoin, are capitalized when referring to the protocol, and lowercase when referring to units of the cryptocurrency.

<sup>6</sup> To the extent this Framework discusses or references criminal cases that are pending at the time of publication, it should be noted that criminal charges are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>7</sup> For example, Christopher Bantli, a Canadian citizen, used cryptocurrency while acting as a vendor of controlled substances on the darknet website AlphaBay. In February 2019, Bantli pleaded guilty in U.S. federal court to accepting virtual currency as payment for controlled substances, including powerful fentanyl analogues and synthetic opiates. See Press Release, "Dark Web Trafficker Convicted of Drug Importation Conspiracy," U.S. DEPT. OF JUSTICE

(Feb. 13, 2019), available at: <https://www.justice.gov/opa/pr/dark-web-trafficker-convicted-drug-importation-conspiracy> (last accessed Oct. 1, 2020).

<sup>8</sup> In October 2018, Ammar Atef Alahdali pleaded guilty to receipt of child pornography after admitting to paying cryptocurrency to become a member of a darknet website dedicated to the advertisement and distribution of such illicit material. In 2017, Alahdali used the website to download more than twenty images depicting the sexual abuse of children, including at least one video depicting sadistic sexual conduct. See Press Release, "Foreign National Pleads Guilty to Downloading Child Pornography from the Dark Web in Exchange for Cryptocurrency," U.S. DEPT. OF JUSTICE (Oct. 2, 2018), available at: <https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-downloading-child-pornography-dark-web-exchange-cryptocurrency> (last accessed Oct. 1, 2020).

<sup>9</sup> For examples of cases where cryptocurrencies were used in the illicit sales on the dark web, see, e.g., *United States v. Hagan*, 766 Fed. Appx. 356 (6th Cir. 2019) (MDMA, LSD, DMT, mushrooms, and marijuana); *United States v. Reuer*, CR. 19-50022-JLV, 2019 WL 1012187 (D.S.D. Mar. 4, 2019) (methamphetamine, fentanyl, and heroin); *State v. Sawyer*, 187 A.3d 377 (Vt. 2018) (firearms); *State v. A.P.*, 117 N.E.3d 840 (Ohio 2018) (LSD); *United States v. 2013 Lamborghini Aventador*, No. 1:17-cv-00967-ljo-sko, 2018 WL 3752131 (E.D. Cal. Aug. 8, 2018) (luxury vehicles); *United States v. Michell*, No. CR-17-01690-001-PHX-GMS, 2018 WL 2688803 (D. Ariz. June 5, 2018) (potassium cyanide and dimethyl mercury); *United States v. Vallerius*, No. 17-CR-20648, 2018 WL 2325729 (S.D. Fla. May 1, 2018) (narcotics); *United States v. Focia*, 869 F.3d 1269 (11th Cir. 2017) (firearms); *United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017) (drugs, false identification documents, and computer hacking software);



*United States v. Colldock*, No. CR-16-1254-JAS, 2017 WL 9615895 (D. Ariz. Sept. 11, 2017) (methamphetamine and cocaine); *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016) (child pornography); *United States v. Parks*, No. S1-4:15 CR 553, 2016 WL 6775465 (E.D. Mo. Sept. 19, 2016) (human trafficking and prostitution); *United States v. 50.44 Bitcoins*, No. ELH-15-3692, 2016 WL 3049166 (D. Md. May 31, 2016) (narcotics and illicit Bitcoin-to-fiat-currency exchanges); and *United States v. Donagal*, No. 14-cr-00285-JST-1, 2014 WL 6601843 (N.D. Cal. Nov. 18, 2014) (illegally manufactured Xanax, GHB, steroids, and other drugs).

<sup>10</sup> See *infra* pages 7-20 (describing AlphaBay, Operation DisrupTor, terrorist financing cases, and other examples).

<sup>11</sup> For example, in 2017, the U.S. government formally asserted that North Korea conducted a massive ransomware attack, referred to as the WannaCry attack, which infected computers around the world. The perpetrators of the WannaCry attack demanded ransom payments from their victims in Bitcoin. See, e.g., Thomas P. Bossert, *It's Official: North Korea Is Behind WannaCry*, WALL ST. J., Dec. 18, 2017, available at: <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537> (last accessed Oct. 1, 2020).

<sup>12</sup> Press Release, "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic," FEDERAL BUREAU OF INVESTIGATION (Apr. 13, 2020), available at: <https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic#:~:text=FBI%20Expects%20a%20Rise%20in%20Scams%20Involving%20Cryptocurrency%20Related%20to,through%20the%20complex%20cryptocurrency%20ecosystem> (last accessed Oct. 1, 2020).

<sup>13</sup> See *infra* page 16.

<sup>14</sup> In what was reported in January 2015 as the "first instance of an ISIS cell fundraising using Bitcoin on the dark web," the FBI shut down the online cryptocurrency account of a known ISIS fundraiser, Abu Mustafa. Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, & Julia Solomon-Strauss, *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, CTR. FOR A NEW AM. SEC., May 2017, at 12, available at: <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf?mtime=20170502033819> (last accessed Oct. 1, 2020); see also European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, *Virtual Currencies and Terrorist Financing: Assessing Risks and Evaluating Responses*, May 2018, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (providing detailed threat assessment, describing European Union's response, and setting out policy recommendations) (last accessed Oct. 1, 2020).

<sup>15</sup> Press Release, "Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL," U.S. DEPT. OF JUSTICE (Aug. 28, 2015), available at: <https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil> (last accessed Oct. 1, 2020).

<sup>16</sup> Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," U.S. DEPT. OF JUSTICE (Aug. 13, 2020), available at: <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns> (last accessed Oct. 1, 2020).

<sup>17</sup> See Press Release, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals,



Municipalities, and Public Institutions, Causing Over \$30 Million in Losses,” U.S. DEPT. OF JUSTICE (Nov. 28, 2018), available at: <https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>18</sup> Press Release, “South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin,” U.S. DEPT. OF JUSTICE (Oct. 16, 2019), available at: <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>19</sup> Indictment, *United States v. Mohammad*, No. 20-cr-0065, at 6 (DLF) (D.D.C. March 2020), available at: <https://www.justice.gov/usao-dc/press-release/file/1257641/download> (last accessed Oct. 1, 2020); *see also* Press Release, “Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 ‘Real Rape’ and Child Pornography Videos, Funded by Cryptocurrency,” U.S. DEPT. OF JUSTICE (Mar. 12, 2020), available at: <https://www.justice.gov/usao-dc/pr/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>20</sup> Verified Complaint for Forfeiture In Rem, *United States v. Three Hundred Three Virtual Currency Accounts et. al.*, No. 20-cv-712 (D.D.C. Mar. 12, 2020), available at: <https://www.justice.gov/usao-dc/press-release/file/1257581/download> (last accessed Oct. 1, 2020).

<sup>21</sup> Press Release, “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns,” *supra* note 16.

<sup>22</sup> Verified Complaint for Forfeiture In Rem, *United States v. One Hundred Fifty Five Virtual Currency Assets*, No. 20-cv-2228 (D.D.C. Aug. 13, 2020), available at: <https://www.justice.gov/opa/press-release/file/1304296/download> (last accessed Oct. 1, 2020).

<sup>23</sup> Press Release, “‘Bitcoin Maven’ Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, C.D. CAL. (July 9, 2018), available at: <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> (last accessed Oct. 1, 2020).

<sup>24</sup> The federal crime of money laundering is defined in 18 U.S.C. § 1956.

<sup>25</sup> AML/CFT standards are discussed further in Part II.

<sup>26</sup> *See* FINCEN GUIDANCE FIN-2013-G001, *supra* note 4, at 2; *see also* VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS, *supra* note 4, at 7.

<sup>27</sup> Press Release, “‘Bitcoin Maven’ Sentenced to One Year,” *supra* note 23.



<sup>28</sup> Press Release, “Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, N.D. CAL. (July 26, 2017), available at: <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>29</sup> For other examples of cases in which virtual currency exchanges have been charged with operating an unlicensed money transmitting business, see *United States v. Murgio*, 15-cr-769(AJN), 2017 WL 365496 (S.D.N.Y. Jan. 20, 2017) and *United States v. Faiella*, 39 F. Supp. 3d 544 (S.D.N.Y. 2014). See also *United States v. Budovsky*, No. 13-cr-368 (DLC), 2015 WL 5602853, at \*14 (S.D.N.Y. Sept. 23, 2015) (noting that 18 U.S.C. § 1960, which covers operation of an unlicensed money transmitting business, encompasses businesses that transmit virtual currency).

<sup>30</sup> See I.R.S. Notice 2014-21, available at: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> (last accessed Oct. 1, 2020).

<sup>31</sup> Press Release, “Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela,” U.S. DEPT. OF THE TREASURY (Mar. 11, 2019), available at: <https://home.treasury.gov/news/press-releases/sm622> (last accessed Oct. 1, 2020).

<sup>32</sup> See generally, e.g., Yaya J. Fanusie & Trevor Logan, *Crypto Rogues: U.S. State Adversaries Seeking Blockchain Sanctions Resistance*, FOUND. FOR DEF. OF DEMOCRACIES (July 2019),

available at: <https://www.fdd.org/wp-content/uploads/2019/07/fdd-report-crypto-rogues.pdf> (last accessed Oct. 1, 2020). While publicly available details remain scarce, reports indicate that North Korea also has been active in exploiting cryptocurrency technology in part because of “a desire to avoid crippling international sanctions.” Megan McBride & Zack Gold, *Cryptocurrency: Implications for Special Operations Forces* at 30, CNA (Aug. 2019), available at: [https://www.cna.org/CNA\\_files/PDF/CRM-2019-U-020186-Final.pdf](https://www.cna.org/CNA_files/PDF/CRM-2019-U-020186-Final.pdf) (last accessed Oct. 1, 2020); see also *Crypto Rogues*, *supra*, at 8 n.4 (“North Korea is also trying to obtain cryptocurrencies to offset sanctions mostly through cyber theft.”).

<sup>33</sup> Gertrude Chavez-Dreyfuss, *Cryptocurrency Crime Losses More than Double to \$4.5 Billion in 2019, Report Finds*, REUTERS, Feb. 11, 2020, available at: <https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-losses-more-than-double-to-45-billion-in-2019-report-finds-idUSKBN2051VT> (last accessed Oct. 1, 2020).

<sup>34</sup> As discussed further in the text, the Department of Justice recently brought criminal charges against two individuals accused of laundering over \$100 million worth of cryptocurrency allegedly stolen by North Korean hacks of cryptocurrency exchanges. The Department also filed a civil forfeiture complaint that “publicly exposes the ongoing connections between North Korea’s cyber-hacking program and a Chinese cryptocurrency money laundering network.” Press Release, “United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors,” U.S. DEPT. OF JUSTICE (August 27, 2020), available at: <https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges> (last accessed Oct. 1, 2020). In April 2020, the U.S. Departments of State, Treasury,



and Homeland Security, along with the Federal Bureau of Investigation, issued an advisory on the cyber threat posed by the North Korean regime. The advisory detailed North Korea's use of state-sponsored cyber actors, including "hackers, cryptologists, and software developers," who, among other things, engage in "cyber-enabled theft targeting financial institutions and digital currency exchanges." U.S. DEPT. OF HOMELAND SEC. ET AL., DPRK CYBER THREAT ADVISORY, *Guidance on the North Korean Cyber Threat* (Apr. 15, 2020), available at: [https://us-cert.cisa.gov/sites/default/files/2020-04/DPRK\\_Cyber\\_Threat\\_Advisory\\_04152020\\_S508C.pdf](https://us-cert.cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf) (last accessed Oct. 1, 2020).

<sup>35</sup> Cryptocurrency Crime Losses, *supra* note 33.

<sup>36</sup> Press Release, "Operator Of Bitcoin Investment Platform Pleads Guilty To Securities Fraud And Obstruction Of Justice," U.S. DEPT. OF JUSTICE, U.S. ATT'Y'S OFFICE, SDNY (July 23, 2018), available at: <https://www.justice.gov/usao-sdny/pr/operator-bitcoin-investment-platform-pleads-guilty-securities-fraud-and-obstruction> (last accessed Oct. 1, 2020).

<sup>37</sup> Press Release, "Trader Sentenced to 15 Months in Federal Prison for Misappropriating \$1.1 Million in Cryptocurrencies," U.S. DEPT. OF JUSTICE, U.S. ATT'Y'S OFFICE, N.D. ILL. (Nov. 13, 2018), available at: <https://www.justice.gov/usao-ndil/pr/trader-sentenced-15-months-federal-prison-misappropriating-11-million-cryptocurrency-0> (last accessed Oct. 1, 2020).

<sup>38</sup> Norton, *What is Cryptojacking? How It Works and How to Help Prevent It*, <https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html> (last accessed Oct. 1, 2020).

<sup>39</sup> The aforementioned April 2020 U.S. government advisory regarding North Korea's cyber-hacking program discussed the regime's

potential involvement in multiple cryptojacking schemes. See DPRK CYBER THREAT ADVISORY, *supra* note 34 at 2. Specifically, the advisory noted "several incidents in which computers infected with cryptojacking malware sent the mined assets—much of it anonymity-enhanced digital currency (sometimes also referred to as 'privacy coins')—to servers located in [North Korea]." *Id.* (citing a report by a UN Security Council panel of experts); see also, e.g., Timothy W. Martin, *New North Korea Hack: Hijacking Computers to Power Cryptocurrency Mining*, WALL ST. J., Jan. 8, 2018, available at: [https://www.wsj.com/articles/in-north-korea-hackers-mine-cryptocurrency-abroad-1515420004?mod=article\\_inline](https://www.wsj.com/articles/in-north-korea-hackers-mine-cryptocurrency-abroad-1515420004?mod=article_inline) (last accessed Oct. 1, 2020).

<sup>40</sup> Press Release, "Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet," U.S. DEPT. OF JUSTICE (May 8, 2019), available at: <https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>41</sup> See Press Release, "3 Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges," U.S. DEPT. OF JUSTICE, U.S. ATT'Y'S OFFICE, C.D. CAL. (May 3, 2019), available at: <https://www.justice.gov/usao-cdca/pr/3-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us> (last accessed Oct. 1, 2020) (describing criminal complaint against the alleged administrators of Wall Street Market (WSM), "one of the world's largest dark web marketplaces that allowed vendors to sell a wide variety of contraband,



including an array of illegal narcotics, counterfeit goods and malicious computer hacking software”).

<sup>42</sup> Press Release, “J-CODE Announces 61 Arrests in its Second Coordinated Law Enforcement Operation Targeting Opioid Trafficking on the Darknet,” FEDERAL BUREAU OF INVESTIGATION (Mar. 26, 2019), available at: <https://www.fbi.gov/news/pressrel/press-releases/j-code-announces-61-arrests-in-its-second-coordinated-law-enforcement-operation-targeting-opioid-trafficking-on-the-darknet> (last accessed Oct. 1, 2020).

<sup>43</sup> Press Release, “International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over \$6.5 Million,” U.S. DEPT. OF JUSTICE (Sept. 22, 2020), available at: <https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170> (last accessed Oct. 1, 2020).

<sup>44</sup> Press Release, “Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet,” U.S. DEPT. OF JUSTICE (May 8, 2019), available at: <https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>45</sup> *Id.*

<sup>46</sup> See 18 U.S.C. §§ 2339A & B.

<sup>47</sup> See 18 U.S.C. § 792 *et seq.*

<sup>48</sup> 31 C.F.R. § 1010.100(ff).

<sup>49</sup> FATF INTERNATIONAL STANDARDS, *supra* note 2, at 127.

<sup>50</sup> As noted above, “AML/CFT” refers to anti-money laundering and combating the financing of terrorism.

<sup>51</sup> Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970). The BSA is the nation’s first and most comprehensive federal AML/CFT statute. The Act, which is codified at 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951–1959, and 31 U.S.C. §§ 5311–5314 and 5316–5332, has been amended at various times, including in October 2001 by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the “USA PATRIOT Act”). Title III of the USA PATRIOT Act amended the BSA to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Regulations implementing all aspects of the BSA appear at 31 C.F.R. Chapter X.

<sup>52</sup> The authority of the Secretary of the Treasury to administer the BSA and its implementing regulations has been delegated to the Director of FinCEN. Pursuant to this delegation, FinCEN, among other things, develops AML regulations and enforces compliance with the BSA and associated regulations. See Treas. Order 180-01 (July 1, 2014), available at: <https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to180-01.aspx> (last accessed Oct. 1, 2020).

<sup>53</sup> See 31 U.S.C. § 310(c); U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF’T NETWORK, What is the BSA Data?, <https://www.fincen.gov/what-bsa-data> (last accessed Oct. 1, 2020).

<sup>54</sup> See EGMONT GRP., *Financial Intelligence Units (FIUs)*, <https://egmontgroup.org/en/content/>



[financial-intelligence-units-fius](#) (last accessed Oct. 1, 2020).

<sup>55</sup> U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FINCEN GUIDANCE FIN-2019-G001, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 7 (May 9, 2019), available at: <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> (last accessed Oct. 1, 2020).

<sup>56</sup> 76 Fed. Reg. 43585 (2011); *see also* 31 CFR § 1010.100(ff)(5)(A) (emphasis added).

<sup>57</sup> 74 Fed. Reg. 22129, 22137 (2009).

<sup>58</sup> Press Release, "FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities," U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, (Mar. 18, 2013), available at: <https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities> (last accessed Oct. 1, 2020).

<sup>59</sup> *See* FinCEN Guidance FIN-2013-G001, *supra* note 4.

<sup>60</sup> *Id.*

<sup>61</sup> *See generally* 31 C.F.R. Part 1022 (setting out BSA requirements applicable to MSBs).

<sup>62</sup> *See* FinCEN Guidance FIN-2019-G001, *supra* note 55.

<sup>63</sup> *See id.* at 12.

<sup>64</sup> *Id.*; *see also* 31 CFR § 1010.100(ff).

<sup>65</sup> The 2013 FinCEN guidance notes that a virtual currency exchanger is a person engaged as

a business in the exchange of virtual currency for real currency, funds, or other virtual currency. *See* FINCEN GUIDANCE FIN-2013-G001, *supra* note 4, at 2. Further, as noted above, an exchanger is a money transmitter if it accepts and transmits a convertible virtual currency or buys or sells convertible virtual currency for any reason. *Id.* at 3; *see also* Kenneth A. Blanco, Director, U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), available at: <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block> (last accessed Oct. 1, 2020).

<sup>66</sup> *See* 31 U.S.C. § 5321 (authorizing the imposition of civil monetary penalties for violations of the BSA); *see also* 31 C.F.R. §§ 1010.820–821.

<sup>67</sup> Press Release, "Ripple Labs Inc. Resolves Criminal Investigation," U.S. DEPT. OF JUSTICE (May 5, 2015), available at: <https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation> (last accessed Oct. 1, 2020); Press Release, "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger," U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK (May 5, 2015), available at: <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual> (last accessed Oct. 1, 2020).

<sup>68</sup> In another example of successful coordination, the Department of Justice in 2017 filed criminal charges against MSB BTC-e and its operator (as discussed above), while FinCEN brought a parallel civil enforcement action. *See* Superseding Indictment, *United States v. BTC-e*, No. CR 16-00227 SI (N.D. Cal. Jan. 17, 2017), available at: <https://www.justice.gov/usao-ndca/press-release/file/984661/download> (last accessed



Oct. 1, 2020); *see also* Press Release, “FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales,” U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF’T NETWORK (July 26, 2017), available at: <https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%2026%20Press%20Release%20FINAL1.pdf> (last accessed Oct. 1, 2020).

<sup>69</sup> *See generally* U.S. DEPT’ OF THE TREASURY, Office of Foreign Assets Control—Sanctions Programs and Information, <https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx> (last accessed Oct. 1, 2020).

<sup>70</sup> OFAC uses the term “digital currency,” which includes cryptocurrency and blockchain-based tokens.

<sup>71</sup> U.S. DEPT’ OF THE TREASURY, Resource Center, OFAC FAQs: Sanctions Compliance, [https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq\\_compliance.aspx](https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx) (last accessed Oct. 1, 2020).

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> OFAC typically uses Executive Orders to designate persons or entities.

<sup>75</sup> Press Release, “Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses,” U.S. DEPT. OF THE TREASURY (Nov. 28, 2018), available at: <https://home.treasury.gov/news/press-releases/sm556> (last accessed Oct. 1, 2020). For further discussion of the SamSam ransomware scheme, *see supra* page 8.

<sup>76</sup> Press Release, “Treasury Designates Iran-Based Financial Facilitators,” *supra* note 75

(“While OFAC routinely provides identifiers for designated persons, today’s action marks the first time OFAC is publicly attributing digital currency addresses to designated individuals. Like traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses.”).

<sup>77</sup> *Id.*

<sup>78</sup> Press Release, “Two Iranian Men Indicted,” *supra* note 17; Indictment, *United States v. Savandi et al.*, No. 18-CR-704 (BRM) (D.N.J. Nov. 26, 2018), available at: <https://www.justice.gov/opa/press-release/file/1114741/download> (last accessed Oct. 1, 2020).

<sup>79</sup> Press Release, “Treasury Targets Chinese Drug Kingpins Fueling America’s Deadly Opioid Crisis,” U.S. DEPT. OF THE TREASURY (Aug. 21, 2019), available at: <https://home.treasury.gov/news/press-releases/sm756> (last accessed Oct. 1, 2020).

<sup>80</sup> Press Release, “Chinese National Indicted in Southern District of Mississippi Designated by U.S. Treasury Department as Significant Foreign Narcotics Trafficker,” U.S. DEPT. OF JUSTICE (Aug 22, 2019), available at: <https://www.justice.gov/usao-sdms/pr/chinese-national-indicted-southern-district-mississippi-designated-us-treasury> (last accessed Oct. 1, 2020).

<sup>81</sup> Press Release, “Two Chinese Nationals Charged with Operating Global Opioid and Drug Manufacturing Conspiracy Resulting in Deaths,” U.S. DEPT. OF JUSTICE (Aug 22, 2018), available at: <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-operating-global-opioid-and-drug-manufacturing-conspiracy> (last accessed Oct. 1, 2020).



<sup>82</sup> Press Release, “Treasury Sanctions Russia-Linked Election Interference Actors,” U.S. DEPT. OF THE TREASURY (Sept. 10, 2020), available at: <https://home.treasury.gov/news/press-releases/sm1118> (last accessed Oct. 1, 2020).

<sup>83</sup> Press Release, “Russian Project Lakhta Member Charged with Wire Fraud Conspiracy,” U.S. DEPT. OF JUSTICE (Sept. 10, 2020), available at: <https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy> (last accessed Oct. 1, 2020); see also Indictment, *United States v. Netyksho et al.*, Case No. 18-cr-00215 (D.D.C. 2018), available at: <https://www.justice.gov/file/1080281/download> (alleging Russian intelligence officers’ use of cryptocurrency to launder funds used in furtherance of U.S. election-related hacking activity) (last accessed Oct. 1, 2020).

<sup>84</sup> See *supra* note 32 and accompanying text.

<sup>85</sup> Press Release, “Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group,” U.S. DEPT. OF THE TREASURY (Mar. 2, 2020), available at: <https://home.treasury.gov/news/press-releases/sm924> (last accessed Oct. 1, 2020).

<sup>86</sup> Press Release, “Two Chinese Nationals Charged with Laundering Over \$100 Million in Cryptocurrency From Exchange Hack,” U.S. DEPT. OF JUSTICE (Mar. 2, 2020), available at: <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack> (last accessed Oct. 1, 2020); Indictment, *United States v. Yinyin*, No. 1:20-cr-00052-TJK (D.D.C. Feb. 27, 2020), available at: <https://www.justice.gov/opa/press-release/file/1253486/download> (last accessed Oct. 1, 2020) (charging two Chinese nationals with conspiracy to launder monetary instruments under 18 U.S.C. § 1956(h) and operating an unlicensed money transmitted business under 18 U.S.C. § 1960(a), and seeking forfeiture under 18

U.S.C. § 982(a)(1) and 21 U.S.C. § 853(p)). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>87</sup> Press Release, “United States Files Complaint to Forfeit 280 Cryptocurrency Accounts,” *supra* note 34.

<sup>88</sup> Press Release, “Two Chinese Nationals Charged with Laundering Over \$100 Million,” *supra* note 86.

<sup>89</sup> Press Release, “United States Files Complaint to Forfeit 280 Cryptocurrency Accounts,” *supra* note 34.

<sup>90</sup> Verified Complaint, *United States v. 280 Virtual Currency Accounts*, Civ. No. 20-2396, at 11–12 (D.D.C. Aug. 27, 2020), available at: <https://www.justice.gov/opa/press-release/file/1310421/download> (last accessed Oct. 1, 2020).

<sup>91</sup> Verified Complaint, *United States v. 113 Virtual Currency Accounts*, Civ. No. 20-606, at 4 (D.D.C. Mar. 2, 2020), available at: <https://www.justice.gov/opa/press-release/file/1253491/download> (last accessed Oct. 1, 2020).

<sup>92</sup> *Id.* at 5.

<sup>93</sup> OFFICE OF THE COMPTROLLER OF THE CURRENCY, *What We Do*, <https://www OCC.treas.gov/about/index-about.html> (last accessed Oct. 1, 2020).

<sup>94</sup> OCC Interpretative Letter #1170, *Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers* (July 22, 2020), available at: <https://www OCC.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf> (last accessed Oct. 1, 2020).



<sup>95</sup> *Id.* at 1.

<sup>96</sup> *Id.* Shortly before this Enforcement Framework was finalized for publication, OCC on September 21, 2020 published an interpretive letter clarifying national banks' and federal savings associations' authority—in certain defined circumstances—to hold “reserves” on behalf of customers who issue certain “stablecoins.” (“Stablecoins” are a type of cryptocurrency designed to have a stable value as compared with other types of cryptocurrency, which frequently experience significant volatility.) OCC’s Sept. 21 letter represents the latest step in the agency’s broader effort to set up systems that will enable banks to adopt cryptocurrency safely. The interpretive letter is available at <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf> (last accessed Oct. 1, 2020).

<sup>97</sup> See OCC Consent Order, *In re M.Y. Safra Bank, FSB*, AA-NE-2020-5, at 3 (Jan. 30, 2020), available at: <https://www.occ.gov/static/enforcement-actions/ea2020-005.pdf> (last accessed Oct. 1, 2020).

<sup>98</sup> U.S. SEC. AND EXCH. COMM’N, RELEASE NO. 81207: REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 10 (July 25, 2017), available at: <https://www.sec.gov/litigation/investreport/34-81207.pdf> (last accessed Oct. 1, 2020).

<sup>99</sup> U.S. SEC. & EXCH. COMM’N STAFF, FRAMEWORK FOR ‘INVESTMENT CONTRACT’ ANALYSIS OF DIGITAL ASSETS, available at: <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets> (last accessed Oct. 1, 2020); FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Initial Coin Offerings*, <https://www.finra.org/>

[investors/learn-to-invest/types-investments/initial-coin-offerings-and-cryptocurrencies/initial-coin-offerings](https://www.finra.org/investors/learn-to-invest/types-investments/initial-coin-offerings-and-cryptocurrencies/initial-coin-offerings) (last accessed Oct. 1, 2020).

<sup>100</sup> The Financial Industry Regulatory Authority (FINRA), which operates under the supervision of the SEC, has issued several investor alerts regarding key cryptocurrency issues, such as ICOs and cryptocurrency-related scams. See, e.g., FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Investor Alert, Initial Coin Offerings (ICOs)—What to Know Now and Time-Tested Tips for Investors*, <https://www.finra.org/investors/alerts/icos-what-know-now> (last accessed Oct. 1, 2020); FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Investor Alert, Don’t Fall for Cryptocurrency-Related Stock Scams*, <https://www.finra.org/investors/alerts/cryptocurrency-related-stock-scams> (last accessed Oct. 1, 2020).

<sup>101</sup> SEC RELEASE NO. 81207, *supra* note 98.

<sup>102</sup> *Id.* at 17–18; see also Jay Clayton [SEC Chairman] and Christopher Giancarlo [CFTC Chairman], *Regulators are Looking at Cryptocurrency*, WALL ST. J., Jan. 24, 2018, available at: <https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363> (“The SEC does not have direct oversight of transactions in currencies or commodities. Yet some products that are labeled cryptocurrencies have characteristics that make them securities. The offer, sale and trading of such products must be carried out in compliance with securities law.”) (last accessed Oct. 1, 2020).

<sup>103</sup> Section 12(k)(1) of the Securities Exchange Act provides the SEC with authority “summarily to suspend trading in any security,” other than certain exempted securities, “for a period not exceeding 10 business days” if doing so is, in the SEC’s opinion, “in the public interest” and required for “the protection of investors.” 15 U.S.C. § 78l(k)(1).



<sup>104</sup> The SEC Staff publishes a list of its digital-asset- and ICO-related enforcement actions on its website. See U.S. SEC. AND EXCH. COMM’N, *Cyber Enforcement Actions*, <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions> (last accessed Oct. 1, 2020); see also U.S. SEC. & EXCH. COMM’N, *Spotlight on Initial Coin Offerings and Digital Assets*, <https://www.investor.gov/additional-resources/spotlight/spotlight-initial-coin-offerings-and-digital-assets> (collecting SEC resources on ICOs and other digital-asset-related issues) (last accessed Oct. 1, 2020).

<sup>105</sup> FRAMEWORK FOR ‘INVESTMENT CONTRACT’ ANALYSIS OF DIGITAL ASSETS, *supra* note 99.

<sup>106</sup> *SEC v. W. J. Howey Co.*, 328 U.S. 293, 301 (1946).

<sup>107</sup> FRAMEWORK FOR ‘INVESTMENT CONTRACT’ ANALYSIS OF DIGITAL ASSETS, *supra* note 99.

<sup>108</sup> The public can engage with SEC Staff through the SEC’s Strategic Hub for Innovation and Financial Technology (FinHub). U.S. SEC. AND EXCH. COMM’N, *FinHub*, [www.sec.gov/finhub](http://www.sec.gov/finhub) (last accessed Oct. 1, 2020).

<sup>109</sup> Press Release, “SEC Halts Alleged \$1.7 Billion Unregistered Digital Token Offering,” U.S. SEC. AND EXCH. COMM’N (Oct. 11, 2019), available at: <https://www.sec.gov/news/press-release/2019-212> (last accessed Oct. 1, 2020).

<sup>110</sup> *Id.*

<sup>111</sup> *Id.*

<sup>112</sup> *Id.* In response, Telegram and TON Issuer argued that the sale of Grams to sophisticated investors were lawful private placements of securities covered by an exemption from the

registration requirement, and that the anticipated resale of the Grams by those investors to a secondary public market, upon the launch of the TON Blockchain, were unrelated transactions that would not amount to the offer or sale of securities. See *SEC v. Telegram Group Inc.*, No. 19-cv-09439-PKC, 2020 WL 1430035, at \*1 (S.D.N.Y. Mar. 24, 2020).

<sup>113</sup> *Id.*

<sup>114</sup> *Id.*

<sup>115</sup> Final Judgment, *SEC v. Telegram Group Inc.*, No. 19-cv-09439-PKC, (S.D.N.Y. June 26, 2020), Dkt. No. 242.

<sup>116</sup> For example, in April 2019, the SEC’s Division of Corporation Finance provided a “no-action letter” in response to an inquiry from TurnKey Jet, Inc., an interstate air charter services company that proposed “to offer and sell blockchain-based digital assets in the form of ‘tokenized’ jet cards” without registering under the Securities Act of 1933 or the Securities Exchange Act of 1934. See Letter from James P. Curry to SEC Office of Chief Counsel (Apr. 2, 2019), available at: <https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1-incoming.pdf> (last accessed Oct. 1, 2020). The no-action letter stated that the Division of Corporation Finance would not recommend enforcement action against the company if, based on the facts presented, it offered and sold tokens without registration. See TurnKey Jet, Inc., SEC No-Action Letter (Apr. 3, 2019), available at: <https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm> (last accessed Oct. 1, 2020).

<sup>117</sup> For examples of prosecutions for securities and other fraud relating to ICOs, see, for example, Press Release, “Brooklyn Businessman Pleads Guilty to



Defrauding Investors through Two Initial Coin Offerings,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, E.D.N.Y. (Nov. 15, 2018) (discussing *United States v. Zaslavskiy*, No. 17 CR 647 (RJD) (E.D.N.Y. 2018)), available at: <https://www.justice.gov/usao-edny/pr/brooklyn-businessman-pleads-guilty-defrauding-investors-through-two-initial-coin> (last accessed Oct. 1, 2020), and Press Release, “Founders Of Cryptocurrency Company Indicted In Manhattan Federal Court With Scheme To Defraud Investors,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, S.D.N.Y. (May 14, 2018), (discussing *United States v. Sharma, et. al.*, No. 18 Cr. 340 (LGS) (S.D.N.Y. 2019)), available at: <https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-company-indicted-manhattan-federal-court-scheme-defraud> (last accessed Oct. 1, 2020).

<sup>118</sup> Press Release, “SEC Halts Alleged Initial Coin Offering Scam,” U.S. SEC. AND EXCH. COMM’N (Jan. 30, 2018), available at: <https://www.sec.gov/news/press-release/2018-8> (last accessed Oct. 1, 2020).

<sup>119</sup> Press Release, “Cryptocurrency CEO Indicted After Defrauding Investors of \$4 Million,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, N.D. TEX. (Nov. 28, 2018), available at: <https://www.justice.gov/usao-ndtx/pr/cryptocurrency-ceo-indicted-after-defrauding-investors-4-million> (last accessed Oct. 1, 2020); Indictment, *United States v. Rice*, No. 3:18-CR-587-K (N.D. Tex. Nov. 20, 2018), available at: <https://www.justice.gov/usao-ndtx/press-release/file/1115456/download> (last accessed Oct. 1, 2020).

<sup>120</sup> Press Release, “Executives Settle ICO Scam Charges,” U.S. SEC. AND EXCH. COMM’N (Dec. 12, 2018), available at: <https://www.sec.gov/news/press-release/2018-280> (last accessed Oct. 1, 2020).

<sup>121</sup> 7 U.S.C. § 1 *et seq.*

<sup>122</sup> These terms are defined in the CFTC’s Glossary. See U.S. COMMODITY FUTURES TRADING COMM’N, *CFTC Glossary*, <https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/CFTCGlossary/index.htm> (last accessed Oct. 1, 2020).

<sup>123</sup> 7 U.S.C. § 1(a)(9).

<sup>124</sup> See *In re Kim*, CFTC No. 19-02, 2018 WL 5993718, at \*3 (Oct. 29, 2018) (consent order) (“Virtual currencies such as Bitcoin and Litecoin are encompassed in the definition of ‘commodity’ under [the CEA].”); *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736, at \*2 (Sept. 17, 2015) (consent order) (“Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.”); *In re TeraExchange LLC*, CFTC No. 15-33, 2015 WL 5658082, at \*3 n.3 (Sept. 24, 2015) (consent order) (“Further, bitcoin is a commodity under Section 1a of the Act, 7 U.S.C. § 1a (2012), and is therefore subject as a commodity to applicable provisions of the [CEA] and [CFTC] Regulations.”).

<sup>125</sup> See *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 217 (E.D.N.Y. 2018) (“Virtual currencies can be regulated by CFTC as a commodity. . . . They fall well-within the common definition of ‘commodity’ as well as the [CEA’s] definition of ‘commodities’ as ‘all other goods and articles . . . in which contracts for future delivery are presently or in the future dealt in.’”); *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, 495–98 (D. Mass. 2018) (applying a categorical approach to interpreting “commodity” under the CEA and determining that a non-bitcoin virtual currency is a “commodity” under the Act).

<sup>126</sup> U.S. COMMODITY FUTURES TRADING COMM’N, *A CFTC PRIMER ON VIRTUAL CURRENCIES* 11 (Oct. 2017), available at: [https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftrc\\_primercurrencies100417.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftrc_primercurrencies100417.pdf) (last accessed Oct. 1, 2020).



<sup>127</sup> See, e.g., *In re Plutus Financial Inc.*, CFTC No. 20-23, 2020 WL 4043709 (July 13, 2020) (consent order); *In re BitFinex Inc.*, CFTC No. 16-19, 2016 WL 3137612 (June 2, 2016) (consent order); *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015) (consent order).

<sup>128</sup> *In re TeraExchange*, CFTC No. 15-33, 2015 WL 5658082 (Sept. 24, 2015) (consent order).

<sup>129</sup> *CFTC v. 1Pool Ltd.*, No. 1:18-cv-2243-TNM, 2019 WL 1605201 (Mar. 4, 2019).

<sup>130</sup> Retail Commodity Transactions Involving Certain Digital Assets, 85 Fed. Reg. 37734 (June 24, 2020) (to be codified at 17 C.F.R. pt. 1).

<sup>131</sup> Press Release, “CFTC Staff Issues Advisory for Virtual Currency Products,” COMMODITY FUTURES TRADING COMM’N (May 21, 2018), available at <https://www.cftc.gov/PressRoom/PressReleases/7731-18> (last accessed Oct. 1, 2020).

<sup>132</sup> See, e.g., *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 217 (E.D.N.Y. 2018); *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, 495–98 (D. Mass. 2018).

<sup>133</sup> Press Release, “CFTC Charges Multiple Individuals and Companies with Operating a Fraudulent Scheme Involving Binary Options and a Virtual Currency Known as ATM Coin,” COMMODITY FUTURES TRADING COMM’N (Apr. 18, 2018), available at: <https://www.cftc.gov/PressRoom/PressReleases/7714-18> (last accessed Oct. 1, 2020).

<sup>134</sup> Press Release, “Federal Court Orders Defendants to Pay More than \$4.25 Million for Fraud and Misappropriation,” COMMODITY FUTURES TRADING COMM’N (Nov. 1, 2019), available at: <https://www.cftc.gov/PressRoom/PressReleases/8069-19> (last accessed Oct. 1, 2020).

<sup>135</sup> See Indictment, *United States v. Kantor*, No. 18-CR-177 (E.D.N.Y. Apr. 10, 2018), available at: <https://www.justice.gov/usao-edny/press-release/file/1053266/download> (last accessed Oct. 1, 2020); Press Release, “Defendant Sentenced to 86 Months in Prison for Defrauding Investors in Binary Options and Cryptocurrency Scheme,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, E.D.N.Y. (July 1, 2019), available at: <https://www.justice.gov/usao-edny/pr/defendant-sentenced-86-months-prison-defrauding-investors-binary-options-and> (last accessed Oct. 1, 2020).

<sup>136</sup> Notice 2014-21, 2014-16 I.R.B. 938, available at: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> (last accessed Oct. 1, 2020).

<sup>137</sup> Since July 2019, the IRS has sent thousands of warning letters to taxpayers “that potentially failed to report income and pay the resulting tax from virtual currency transactions or did not report their transactions properly.” News Release, “IRS has Begun Sending Letters to Virtual Currency Owners Advising Them to Pay Back Taxes, File Amended Returns; Part of Agency’s Larger Efforts,” INTERNAL REVENUE SERV. (July 26, 2019), available at: <https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts> (last accessed Oct. 1, 2020).

<sup>138</sup> “A John Doe summons is a summons that does not identify the person with respect to whose liability the summons is issued.” INTERNAL REVENUE MANUAL, Part 25.5.7, *Special Procedures for John Doe Summonses*, available at: [https://www.irs.gov/irm/part25/irm\\_25-005-007](https://www.irs.gov/irm/part25/irm_25-005-007) (last accessed Oct. 1, 2020). The IRS can use John



Doe summonses, which require court approval, in certain circumstances “to obtain information about possible violations of internal revenue laws by individuals whose identities are unknown.” Press Release, “Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency,” U.S. DEPT. OF JUSTICE (Nov. 30, 2016), available at: <https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used> (last accessed Oct. 1, 2020).

<sup>139</sup> Rev. Rul. 2019-24, 2019-44 I.R.B. 1004, available at: <https://www.irs.gov/pub/irs-drop/rr-19-24.pdf> (last accessed Oct. 1, 2020).

<sup>140</sup> INTERNAL REVENUE SERV., Frequently Asked Questions on Virtual Currency Transactions, <https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions> (last accessed Oct. 1, 2020).

<sup>141</sup> *Id.*

<sup>142</sup> N. AM. SEC. ADM’RS ASS’N, *Our Role*, <http://www.nasaa.org/about-us/our-role/> (last accessed Oct. 1, 2020).

<sup>143</sup> NASAA, which is comprised of State and territorial securities regulators, has taken an active role in investor education and in coordinating State actions involving VASPs and ICOs. *See, e.g.*, N. AM. SEC. ADM’RS ASS’N, INFORMED INVESTOR ADVISORY: INITIAL COIN OFFERINGS (Apr. 2018), available at <https://www.nasaa.org/44836/informed-investor-advisory-initial-coin-offerings/?qoid=investor-education> (last accessed Oct. 1, 2020).

<sup>144</sup> News Release, “State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown,” N. AM. SEC. ADM’RS ASS’N (May 21, 2018), available at: <http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/> (last accessed Oct. 1, 2020).

[org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/](http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/) (last accessed Oct. 1, 2020).

<sup>145</sup> *See* N.Y. STATE OFFICE OF THE ATT’Y GEN., VIRTUAL MARKETS INTEGRITY INITIATIVE REPORT (Sept. 18, 2018), available at: <https://virtualmarkets.ag.ny.gov/> (last accessed Oct. 1, 2020).

<sup>146</sup> Press Release, “A.G. Schneiderman Launches Inquiry into Cryptocurrency ‘Exchanges,’” N.Y. STATE OFFICE OF THE ATT’Y GEN. (Apr. 17 2018), available at: <https://ag.ny.gov/press-release/ag-schneiderman-launches-inquiry-cryptocurrency-exchanges> (last accessed Oct. 1, 2020).

<sup>147</sup> The FATF is also known by its French name, Groupe d’action financière (or “GAFI”).

<sup>148</sup> FINANCIAL ACTION TASK FORCE, *What Do We Do*, <http://www.fatf-gafi.org/about/whatwedo/> (last accessed Oct. 1, 2020).

<sup>149</sup> FATF INTERNATIONAL STANDARDS, *supra* note 2, Recommendation 15.

<sup>150</sup> *See id.* at 70–71.

<sup>151</sup> The FATF has undertaken a 12-month review and committed further to a 24-month review of countries’ progress with implementing the revised requirements for VASPs. The FATF’s 12-month review concluded that there has been progress in implementation of the standards, but that much more remains to be done globally by individual jurisdictions. The report further determined that, while there is no need to revise the standards, there is a need for updated guidance, which the FATF plans to release in 2021. The FATF also undertook a report on so-called “stablecoins” at the request of the G20. This report also found no need to update the FATF standards, but did identify a number of concerns that will be addressed in forthcoming guidance.



<sup>152</sup> See 31 C.F.R. §§ 1010.100(ff), 1022.380; *see also* U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FINCEN ADVISORY FIN-2012-A001: FOREIGN-LOCATED MONEY SERVICES BUSINESSES (Feb. 2012), available at: <https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A001.pdf> (last accessed Oct. 1, 2020); U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 F.R. 43585 (July 21, 2011), available at <http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf> (last accessed Oct. 1, 2020).

<sup>153</sup> Many P2P exchange platforms also offer wallet and escrow services, advertising for buyers and sellers, and messaging or chat functions. Generally, platforms that offer hosted wallet services also are MSBs and must comply with the relevant regulations.

<sup>154</sup> See 31 U.S.C. §§ 5318 & 5322.

<sup>155</sup> See *supra* Part I at page 14 (discussing KYC requirements).

<sup>156</sup> Press Release, "O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit," U.S. DEPT. OF JUSTICE, U.S. ATT'Y'S OFFICE, C.D. CAL. (July 22, 2020), available at: <https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin-and> (last accessed Oct. 1, 2020).

<sup>157</sup> 31 C.F.R. 1010.100(t)(5)(i).

<sup>158</sup> See Press Release, "Ohio Resident Charged with Operating Darknet-Based Bitcoin 'Mixer,' which Laundered Over \$300 Million," U.S. DEPT. OF JUSTICE (Feb. 13, 2020), available at: <https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million>

[www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million](https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million) (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<sup>159</sup> 18 U.S.C. § 1956(a)(1)(B)(i).

<sup>160</sup> Verified Complaint, *United States v. 280 Virtual Currency Accounts*, *supra* note 90, at 11.

<sup>161</sup> Last year, the Law Library of Congress published a comprehensive report on over 40 international jurisdictions' regulatory approaches to cryptoassets, focusing on those jurisdictions' financial market and investor protection laws, as well as on their application of tax and AML/CFT laws. That report confirms the vast diversity of domestic virtual currency regulation, and practice, across the globe. See LAW LIBRARY OF CONGRESS, *Regulatory Approaches to Cryptoassets in Selected Jurisdictions* (April 2019), available at: <https://www.loc.gov/law/help/cryptoassets/cryptoasset-regulation.pdf> (last accessed Oct. 1, 2020).

<sup>162</sup> See, e.g., *United States v. Lord*, 915 F.3d 1009 (5th Cir. 2019); *United States v. Stetkiw*, No. 18-20579, 2019 WL 417404 (E.D. Mich. Feb. 1, 2019); *United States v. Tetley*, No. 17-cr-00738 (C.D. Cal. 2018); *United States v. Mansy*, No. 2:15-cr-198-GZS, 2017 WL 9672554 (D. Maine May 11, 2017); *United States v. Petix*, No. 15-CR-227A, 2016 WL 7017919 (W.D.N.Y. Dec. 1, 2016); *United States v. Noland et al.*, 14-cr-00401-RM (D. Col. 2015); *see also* Press Release, "Bitcoin Maven' Sentenced to One Year," *supra* note 23.

<sup>163</sup> *United States v. Al Kassar*, 660 F.3d 108, 118 (2d Cir. 2011) (citing *United States v. Peterson*, 812 F.2d 486, 494 (9th Cir. 1987)).



<sup>164</sup> For more on the concept of protective jurisdiction in the context of U.S. material support statutes, see John De Pue, *Extraterritorial Jurisdiction and the Material Support Statutes*, U.S. ATTY'S BULLETIN, Sept. 2014, available at: <https://www.justice.gov/sites/default/files/usao/legacy/2014/09/23/usab6205.pdf> (last accessed Oct. 1, 2020).

<sup>165</sup> See *supra* Part I at page 14.

<sup>166</sup> See *supra* Part I at 18, 19.

<sup>167</sup> Verified Complaint for Forfeiture *In Rem*, *United States v. Cazes*, No. 1:17-at-00557, at 21 (E.D. Cal. July 19, 2017), available at: <https://www.justice.gov/opa/press-release/file/982821/download> (last accessed Oct. 1, 2020).

<sup>168</sup> Press Release, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," U.S. DEPT. OF JUSTICE (July 20, 2017), available at: <https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down> (last accessed Oct. 1, 2020).

<sup>169</sup> These criminal charges included: narcotics conspiracy (21 U.S.C. §§ 846 and 841(a)(1), (b)(1)(A), (b)(1)(C), 841(h), and 843(b)); distribution of a controlled substance (21 U.S.C. §§ 841(a)(1), (b)(1)(C), & 846); conspiracy to commit identity theft and fraud (18 U.S.C. § 1028(f)); unlawful transfer of a false identification document (18 U.S.C. § 1028(a)(2), (b)(1)(A)(ii), & (f)); conspiracy to commit access device fraud (18 U.S.C. § 1029(b)(2)); trafficking in device making equipment (18 U.S.C. § 1029(a)(4), (b)(1), & (c)(1)(A)(ii)); and money laundering conspiracy (18 U.S.C. § 1956(h)). See Indictment, *United States v. Cazes*, Case No. 1:17-CR-00144 (E.D. Cal. June 1, 2017), available at: <https://www.justice.gov/opa/press-release/file/982826/download> (last accessed Oct. 1, 2020). In addition, prosecutors used various

criminal forfeiture statutes (18 U.S.C. §§ 982(a)(1) and 982(a)(2)(B) and 21 U.S.C. § 853(a)). *Id.*

<sup>170</sup> Verified Complaint, *United States v. 280 Virtual Currency Accounts*, *supra* note 90, at 11.

<sup>171</sup> U.S. DEPT. OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 100-01 (July 2018), available at: <https://www.justice.gov/cyberreport> (last accessed Oct. 1, 2020).

<sup>172</sup> *Id.* at 101.

<sup>173</sup> Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 6.1(c) & (f), available at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679> (last accessed Oct. 1, 2020).

<sup>174</sup> *Id.*, art. 49.1 & 49.1(d).

<sup>175</sup> Br. of the European Comm'n on Behalf of the E.U. as Amicus Curiae in Support of Neither Party, *United States v. Microsoft*, No. 17-2 (U.S. 2018), available at: [https://www.supremecourt.gov/tPDF/17/17-2/23655/20171213123137791\\_17-2%20ac%20European%20Commission%20for%20filing.pdf](https://www.supremecourt.gov/tPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf) (last accessed Oct. 1, 2020).

<sup>176</sup> *Id.* at 15.

<sup>177</sup> General Data Protection Regulation, art. 49.1(e), *supra* note 173

# EXHIBIT 184



# Ethereum Name Service (ENS): Everything You Need To Know

 beincrypto.com/learn/ethereum-name-service-ens/

May 12, 2022

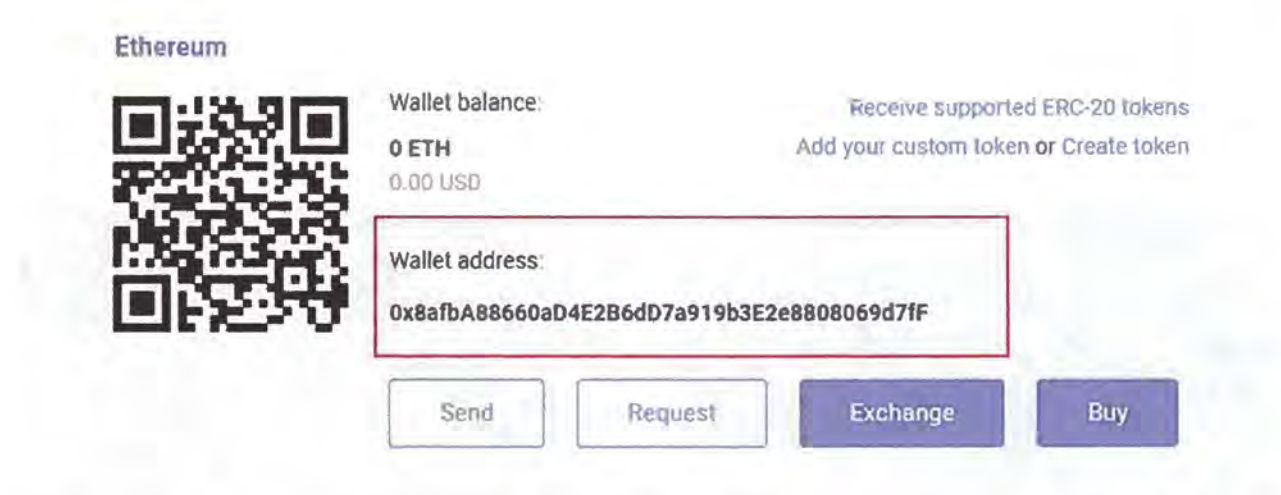


Ethereum Name Service (ENS) is a naming protocol that **allows humans to use easy-to-remember domain names for their cryptocurrency addresses**. The protocol then translates it to a machine-readable address. This process has many similarities to the DNS system we use for the internet. Furthermore, it empowers users with a tool that can unify their online presence and help them step into the realm of web3.

ENS could make all the difference in how we interact in the web3 world. We explain why this might be the case in this guide.

## Ethereum wallet addresses can be inconvenient





Just like internet protocol addresses, blockchain **addresses for cryptocurrency wallets are hard to use by the average user**. Luckily, computer scientists have developed domain names by investing in the Domain Name System (DNS), which allows linking human-readable domain names to IP addresses.

Sponsored  
Sponsored

**DNS matches IP addresses with human-readable DNS names.** Instead of typing 172.64.147.202 into your address box, type beincrypto.com, and you will be taken to the website.

Despite all the technological advancements in the blockchain and crypto sector, the system still uses a system similar to the old IP address setup. **To send crypto to someone else, you will need their cryptocurrency wallet address**, which is a long string of characters. To remember that address is highly unlikely, and it's also not advisable since blockchain transactions are irreversible. **That means that if you send funds to the wrong address, you will never not get it back.**

To better understand the difficulty of the task, here's what an Ethereum (ETH) address looks like: **0xd0eAf74B8c5bF457C7a81c3fe277aDb6Ed32DCF4**

Sponsored Sponsored

**It's a 42-character long string**, and it is commonly referred to as a public address of a cryptocurrency wallet. You can recognize Ethereum network addresses because they **always start with "0x"**.

The main issues with having and using a blockchain address are related to the difficulty of sharing it with others and **the high risk of mistyping a cryptocurrency wallet address** and thus losing your funds. Furthermore, it's important to acknowledge that most cryptocurrency



users are still new to the technology and are just starting to explore it. Having to deal with long strings of characters will probably put off some of them, out of the fear of making a mistake.

This is where the Ethereum Name Services (ENS) comes in.

Sponsored Sponsored

## What is the Ethereum Name Service?



The Ethereum Name Service is an open, distributed, and extensible naming system that interacts directly with the Ethereum blockchain.

Similar to the DNS role, the **ENS has the role of a domain name service that maps human-readable addresses** such as "name.eth," to a machine-readable address such as this long hexadecimal string: "0xd0eAf74B8c5bF457C7a81c3fe277aDb6Ed32DCF4."

The personalized ENS addresses allow users to manage their cryptocurrency funds and assets by simply using a human-friendly domain name. ENS domains aim to become the usernames of web3, and **it can store crypto wallets, websites, content hashes, and metadata**. Owners can connect all their crypto wallets under one single ENS domain and receive cryptocurrencies or NFTs.

Sponsored Sponsored

This means that transactions are secure and decentralized without the need for lengthy and complicated addresses. This **reduces the chance of making mistakes** when entering the address of the recipient to which funds are sent.

Although the ENS may be identical to the DNS system of the 1980s, its architecture is different.



The ENS is similar to the DNS in that it uses a system called domains. **The domain's creator or owner has control over the top-level domain as well as any subdomains.**

Sponsored Sponsored

Anybody can acquire ownership of domains for their own personal use. ENS supports the import of DNS names that are already owned by users for use on ENS. Due to the hierarchical nature of ENS, **anyone can create subdomains for themselves or others.** For instance, you can create "pay.name.eth" if you own "name.eth" and make any configurations you like.

ENS can be deployed on both the Ethereum main network as well as several test networks.

## **The ENS team**

---

**The initial development of the ENS was led by Alex Van de Sande and Nick Johnson** of the Ethereum Foundation in 2017. But in 2018, it separated into a different organization led by Nick Johnson.

**True Names LTD manages the development of ENS**, a Singaporean non-profit organization. The ENS team consists of experienced Solidity developers, as well as some who used to work with the Ethereum Foundation.

The project distributed ENS tokens to the users of the service in Nov. 2021 and created a decentralized autonomous organization (DAO) to manage it. True Names Limited is the legal entity that connects to the DAO. ENS token-holders can use their assets in the same way as company shareholders; they have the ability to make decisions about pricing and protocol changes, as well managing funds within the Treasury.

The addition of ENS tokens to the project's funding model allowed it to transition away from grants. The ENS tokens can be traded for U.S. Dollars and other cryptocurrencies on crypto exchanges. This provides a financial support system to the developers of the project.

## **The ENS Foundation**

---

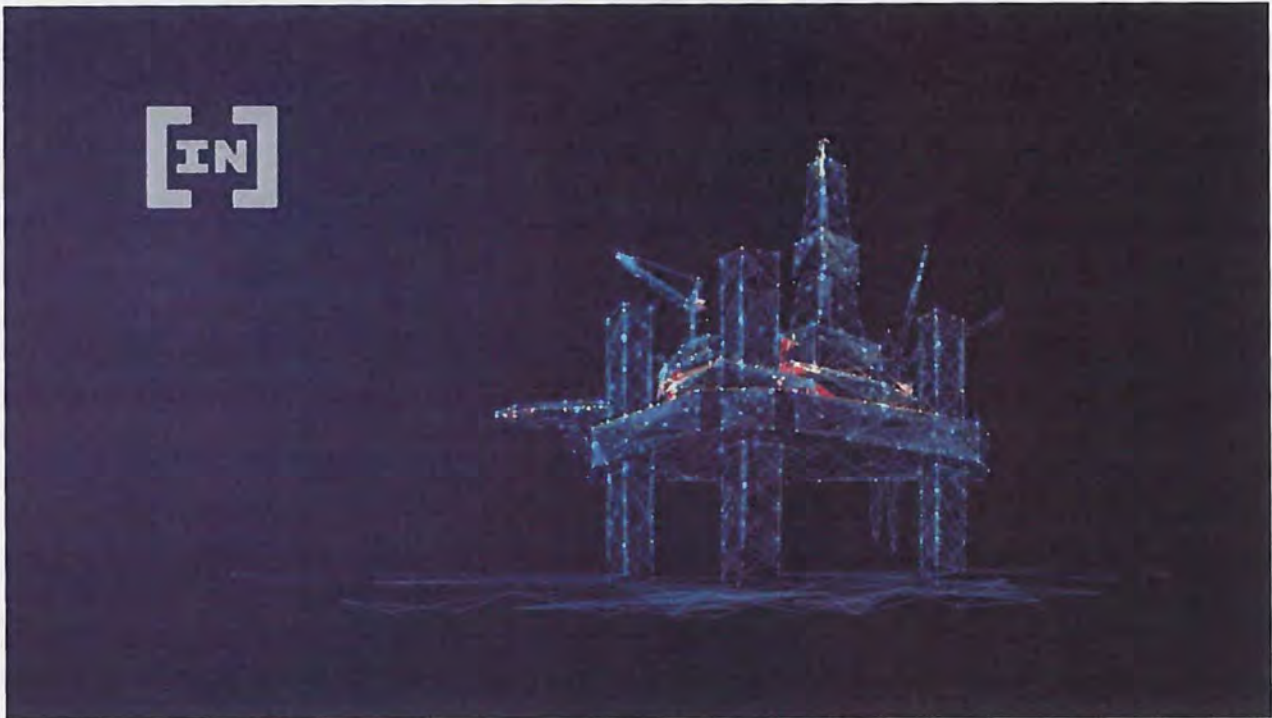
**The ENS DAO is represented by the ENS Foundation.** The foundation is able to provide legal support for DAO participants.

The ENS Foundation, a foundation limited by guarantee, is registered in the Cayman Islands. It is a non-profit and does not pay dividends to its members or directors. One supervisor is appointed by DS Limited, a Cayman Islands company.

More details about the ENS DAO and how the ENS foundation operates can be found on the ENS documentation page.

## **What makes ENS stand out?**





**The ENS domain name is your IBAN equivalent**, which allows others to send cryptocurrency to your wallet. Using ENS, you can create a “nickname” for your public address. This means that instead of sharing a long string of characters with a friend, you will have a link like “Julia.eth,” which is automatically connected to your public address.

**The ENS was created for Ethereum smart contracts** and is native to the Ethereum ecosystem. It doesn’t have the security problems that a DNS system has. The DNS records for domain names and names are kept on a central server. They are vulnerable to hackers. There are thousands of attacks on DNSs and internet providers every year.

However, **ENS records can’t be hacked or deleted** and are protected by the Ethereum Blockchain.

Moreover, by using an ENS domain, the entire interaction between users becomes more transparent and easier to follow. This gives users of the Ethereum blockchain the unique opportunity to open a wallet and stand out from the other addresses.

## **How ENS fares against DNS**

Both the Domain Name System (DNS) and the Ethereum Name Service (ENS) are protocols that can handle human interactions with web2 and web3. DNS converts an IP address into a human-readable string known as a URL.



The Ethereum Name Service (ENS) converts an Ethereum address into a human-readable string formatted as a URL. Both functions are similar to a phone book. It is possible to look up a person's name in a phone book and find the number that allows you to contact them.

Web2 can work seamlessly with the DNS as part of a network of internet protocols. Web3, the concept that describes the new, decentralized internet, is still in its infancy and faces many challenges.

ENS's primary purpose is to make web3 easier to understand and to share crypto addresses. As time passes, more blockchain protocols will support and integrate ENS as part of their web3 integration.

## Ethereum Name Service vs. Unstoppable Domains

---



Of course, there is another foundation that aims to simplify the way humans interact with blockchain addresses. **The main competitor of ENS is Unstoppable Domains**, which also offers transferable domains.

Both Unstoppable Domains, as well as ENS, are built on the Ethereum blockchain. They both allow users to create and register a human-readable crypto address.

There are, however, some significant differences in the philosophy behind these projects. ENS is an open protocol that is visible to the public. Developed by a non-profit organization, it focuses on community decision-making and decentralization.



**Unstoppable Domains is a business-oriented project.** Many domains are “brand protected” to stop individuals from owning specific names, words, or phrases. Some individuals have complained that they are unable to purchase domains with their names, even though the domain isn’t in use.

One big difference between ENS and Unstoppable domains is the payment method. ENS domains allow purchases for a limited period of time, just like normal website domains, and you have to renew your domain each time it expires. Since you will have to use Ethereum (ETH) to pay for the ENS domain and have fees, the prices will differ depending on the moment you want to buy the domain.

However, you can secure your ENS domain for many years and only pay the gas fee once, during registration. Another interesting aspect is that anyone can extend the registration of your ENS domain, but this doesn’t give ownership over your domain.

**Unstoppable Domains need to be registered only once**, and there is no expiration date for your domain. Also, they allow multiple payment options (credit/debit card, PayPal, crypto, and through the Crypto.com app).

## **What makes ENS special**

---

The ENS is built using Ethereum’s smart contract and inherits all benefits of the network. This makes it more secure and private and resists censorship than the internet Domain Name Service (DNS).

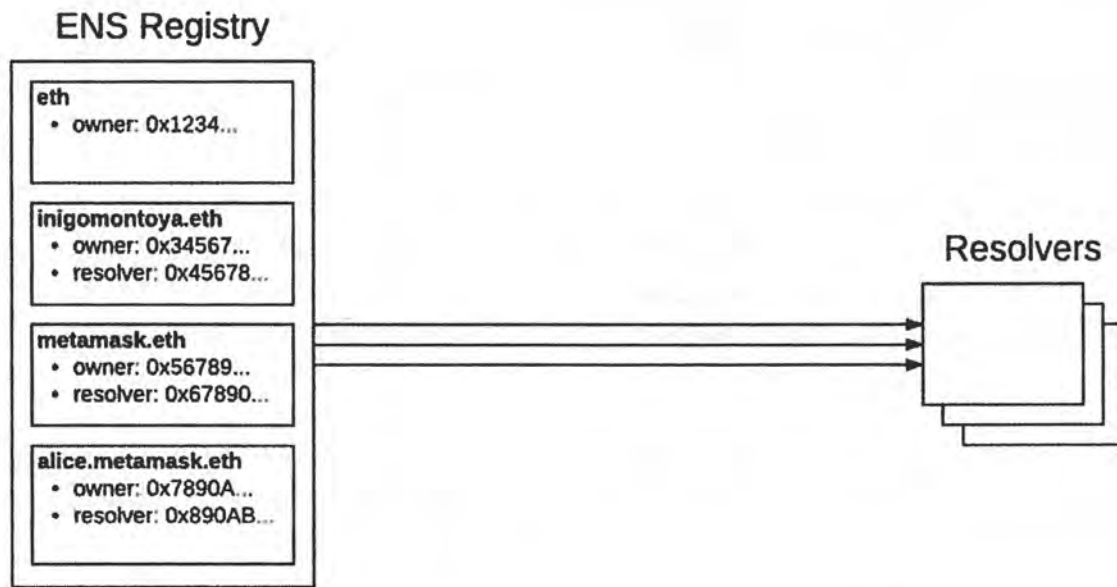
The future web3 aims to be a decentralized and open infrastructure, and it only makes sense when using internet-naming infrastructure such as ENS domains. Since ENS uses the existing Ethereum ecosystem, it can easily interact with other smart contracts and applications built on Ethereum.

The main advantages of having and using an ENS domain are:

- Have multiple web services combined into one
- Unify your online presence
- Central user-owned storage identity
- ENS is a router for non-Ethereum addresses too, like BTC, LTC, etc.
- The ENS name can be linked to a contract address and trigger a function when funds are received
- The ENS domain is linkable to [IPFS](#) to actually host a censorship-resistant website behind the ENS name
- Users can have subdomains linked to different addresses for different purposes

## **How the ENS works**

---



ENS is built upon two Ethereum smart contracts. The first one is the ENS registry, which records all domains registered on ENS. It also stores three crucial pieces of information about each domain. These are the domain owner, resolver, and caching time.

The **resolver** is the second smart contract. It converts domain names into machine-readable addresses and vice versa. This smart contract matches each domain with the appropriate user, website, or address.

## How to get your own ENS domain

The screenshot shows the ENS domain registration interface for 'vasileiulia.eth'. At the top, there is a 'Register' button. Below it, the price is listed as 0.003 ETH for 1 year. A note indicates that the registration is for 1 year to avoid paying gas every year. The total cost, including a gas fee of at most 0.081 ETH, is 0.084 ETH, which is equivalent to \$162.71 USD. A 'Notify Me' button is also present. The registration process is outlined in three steps: 1. Request to register (wallet opens, user confirms first transaction), 2. Wait for 1 minute (waiting period to ensure no one else registers the same name), and 3. Complete Registration (click 'register', wallet re-opens, user confirms second transaction). A note at the bottom states that insufficient balance in the wallet will result in the page being reloaded.

To create your web3 username, you need to have an Ethereum wallet — such as MetaMask — and visit the ENS domains web app. First, search for a domain name. After finding one, you will need to complete the registration process. This includes verifying two transactions



from your wallet and paying **the annual fee of \$5/year**, if the name is longer than five characters. Once you have the domain, you can link it with your crypto wallets and websites.

You can also create multiple subdomains like email.rick.eth and website.rick.eth under the same ENS domain. Note that each modification happens directly on the Ethereum blockchain and will incur a gas fee, which may vary depending on the day and time of the day you're trying to modify your details.

**It's also worth noting that ENS domains are scarce**, and the process is very similar to how you would purchase a DNS name. Since this is still a new side of web3, some crypto enthusiasts purchase multiple ENS domains, hoping to flip them later, when more people and brands get into web3. For instance, "exchange.eth" has sold for 6,660 ETH, and "weather.eth" sold for 300 ETH.

The ENS register also supports most popular DNS names such .com, .org, .io, .app and many more.

## **What is the ENS governance token?**

---

ENS is an open-source protocol that is fully decentralized. It is community-governed by a DAO, which consists of community members that hold ENS tokens.

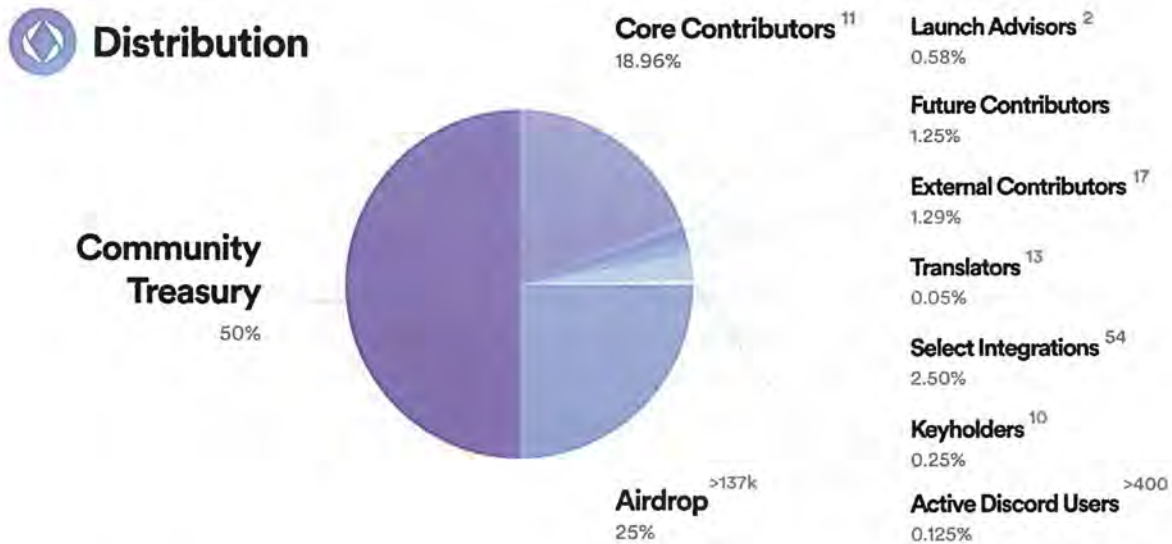
**The ENS DAO is completely governed and controlled by the community** using the ENS token. This token is the utility token and governance token that allows users to submit proposals and vote to shape the future direction of the protocol. Anybody can vote for proposals on the ENSDAO if they hold ENS tokens. As with any DAO, no changes in the protocol can be made without a governance vote.

## **ENS tokenomics**

---

**ENS governance token is an ERC-20 token.** The maximum supply is 100 million ENS tokens.

To distribute ENS to the community, developers allocated 25% to users who had signed up for an ENS domain before Oct. 31, 2021.



Token distribution:

- 50% Community treasury (ENS DAO)
- 25% Airdrop to .eth holders
- 25% ENS contributors

The developers distributed the tokens to wallets that had ENS domains. The allocations were based on the length of time an ENS domain was owned by a user.

This means that casual users were able to receive tokens worth tens of thousands of dollars in the airdrop, while domain owners who have been around for a long time received much larger allocations.

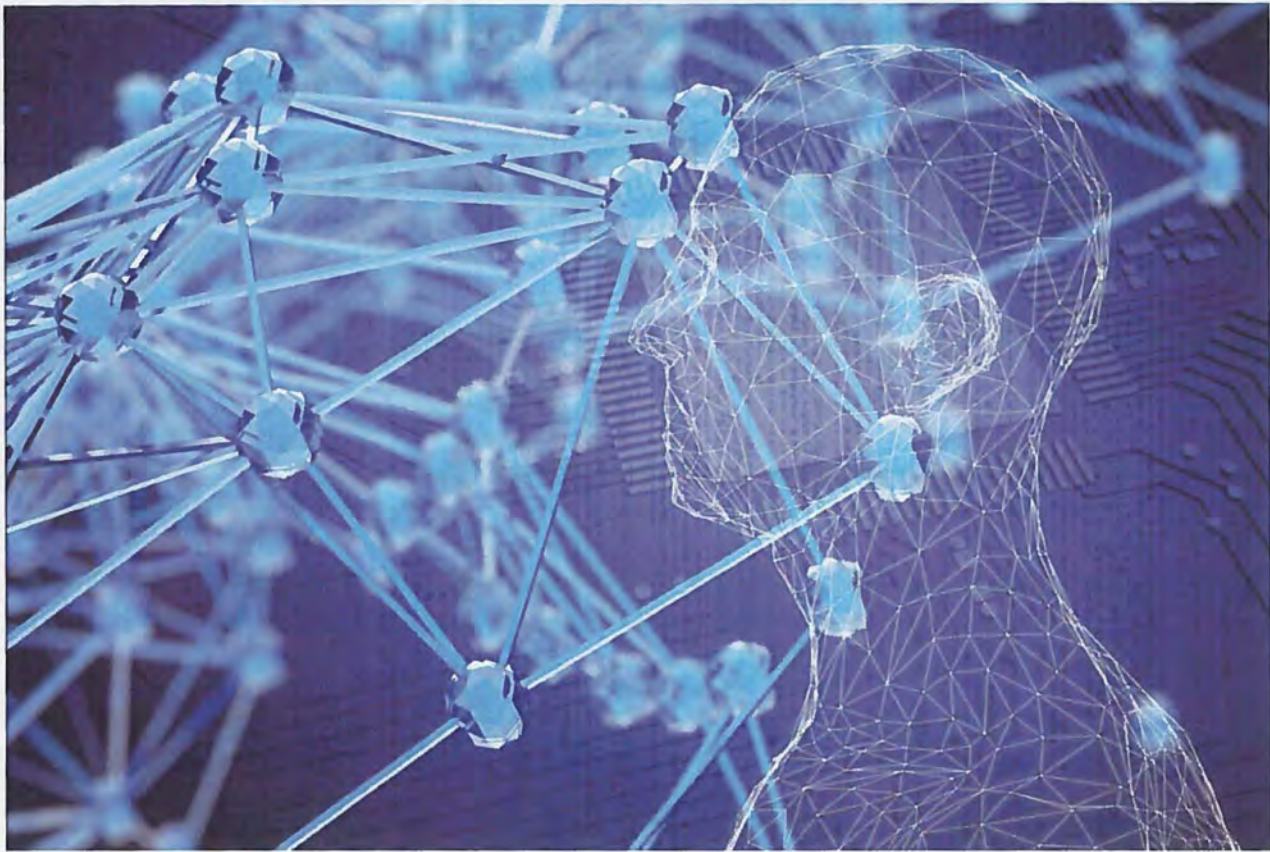
As of May 2022, the circulating supply is at around 20.24 million ENS. Currently, the token is trading at around \$14, and the market cap is \$279.6 million. According to WalletInvestor, the price of ENS might drop and reach \$1.16 by the end of 2022 and \$0.40 by the end of 2027.

ENS is available on the most popular centralized cryptocurrency exchanges, including Binance, Coinbase, Kraken, and others. It is also on DEXs such as Uniswap and SushiSwap.

## What can you do with ENS?

---





The main thing cryptocurrency users can use ENS for is to **replace their long addresses with human-readable domains** that will facilitate crypto operations. Humans can easily remember an ENS that is something like “name.eth,” but will find it almost impossible to remember a string like “0xd0eAf74B8c5bF457C7a81c3fe277aDb6Ed32DCF4.”

At the same time, this will save them time and potential mistyping when connecting to a new DApp that requires them to input their wallet’s address.

ENS domains personalize details of wallets, and this will make it easier for anyone looking to transfer your funds or any other details such as your website or social media handle. This feature can limit the fraudulent attempts of others trying to impersonate you and steal funds from your friends or collaborators.

## **ENS could be at the heart of web3**

---

The ENS was created for Ethereum smart contracts and is native to the Ethereum ecosystem. This means that it inherits its security and transparency, as opposed to the DNS records that are kept on central servers that remain vulnerable to hackers.

Cryptography is complex and can discourage beginners from getting involved. **ENS eliminates this barrier to adoption** by making crypto easier and more accessible. ENS converts the machine-readable public addresses into short, memorable links, which allow



transactions and interactions with any cryptocurrency or NFT. It aims to link all wallets, websites, and subdomains under one link, making crypto more accessible and less technical.

As blockchain addresses become more accessible to new cryptocurrency users, we might see an overall increase in adoption over the long run. For global crypto adoption to be successful, ENS and other similar incentives are crucial.

## **Frequently asked questions**

---

### **What is the difference between ETH and ENS?**

---

Ethereum (ETH) is the native asset of the Ethereum blockchain. ENS is a naming protocol built on the Ethereum blockchain that maps out Ethereum crypto addresses to human-readable domains such as "name.eth."

### **What is ENS crypto?**

---

The ENS is the governance and utility token for the Ethereum Name Service (ENS) and its DAO. ENS token holders can submit proposals and vote on proposals that dictate the future of ENS.

### **Where can I buy Ethereum Name Service (ENS)?**

---

You can buy Ethereum Name Service (ENS) tokens on all major cryptocurrency exchanges such as Binance, Coinbase, or KuCoin. You can also find it on decentralized exchanges (DEXs) such as Uniswap and SushiSwap.

### **How do ETH domains work?**

---

You can buy ETH domains from Ethereum Name Service (ENS), and they act as a human-readable domain name for your cryptocurrency public key, aka wallet address. The ENS Resolver translates ENS names into machine-readable addresses. You can use it to receive



crypto funds and also have all your different crypto addresses stored under the same ENS domain, as well as website addresses and social media handles.

## **How much does an ENS name cost?**

---

There are three tiers for yearly reveals for ENS domains, and it depends on the length of your ENS name. Three character names cost \$640/year, four-character names cost \$160/year, and five character names or longer cost \$5/year. However, users have to pay an Ethereum gas fee each time they renew their ENS. That's why it would be cheaper to register your ENS for a longer period of time, as you would have to pay the gas fee only once.

## **When did Ethereum Name Service start?**

---

Alex Van de Sande and Nick Johnson from the Ethereum Foundation launched Ethereum Name Service (ENS) on May 4, 2017.

## **Disclaimer**

---

All the information contained on our website is published in good faith and for general information purposes only. Any action the reader takes upon the information found on our website is strictly at their own risk. At Learn, our priority is to provide high quality information. We take our time to identify, research and create educative content that is useful to our readers. To maintain this standard and to continue creating awesome content, our partners might reward us with a commission for placements in our articles. However, these commissions don't affect our processes for creating unbiased, honest and helpful content.

Sponsored

# EXHIBIT 199



## Harvard Law School Forum on Corporate Governance

### An Introduction to Smart Contracts and Their Potential and Inherent Limitations

Posted by Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher & Flom LLP, on Saturday, May 26, 2018

**Tags:** Blockchain, Contracts, Cybersecurity, Financial technology, Legal systems, Risk, Risk management

**More from:** Alex Lipton, Stuart Levi, Skadden

**Editor's Note:** Stuart D. Levi is a partner and Alex B. Lipton is an associate at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on their Skadden publication.

"Smart contracts" are a critical component of many platforms and applications being built using blockchain or distributed ledger technology. Below, we outline the background and functions of smart contracts, discuss whether they can be deemed enforceable legal agreements under contract law in the United States, and highlight certain legal and practical considerations that will need to be resolved before they can be broadly used in commercial contexts.

### An Introduction to Smart Contracts

#### How Smart Contracts Function

"Smart contracts" is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform. As discussed further below, the code can either be the sole manifestation of the agreement between the parties or might complement a traditional text-based contract and execute certain provisions, such as transferring funds from Party A to Party B. The code itself is replicated across multiple nodes of a blockchain and, therefore, benefits from the security, permanence and immutability that a blockchain offers. That replication also means that as each new block is added to the blockchain, the code is, in effect, executed. If the parties have indicated, by initiating a transaction, that certain parameters have been met, the code will execute the step triggered by those parameters. If no such transaction has been initiated, the code will not take any steps. Most smart contracts are written in one of the programming languages directly suited for such computer programs, such as Solidity.

At present, the input parameters and the execution steps for a smart contract need to be specific and objective. In other words, if "x" occurs, then execute step "y." Therefore, the actual tasks that smart contracts are performing are fairly rudimentary, such as automatically moving an amount of cryptocurrency from one party's wallet to another when certain criteria are satisfied. As the adoption of blockchain spreads, and as more assets are tokenized or go "on chain," smart contracts will become increasingly complex and capable of handling sophisticated transactions. Indeed, developers already are stringing together multiple transaction steps to form more complex smart contracts. Nonetheless, we are, at the very least, many years away from code being able to determine more subjective legal criteria, such as whether a party satisfied a commercially reasonable efforts standard or whether an indemnifications clause should be triggered and the indemnity paid.

Before a compiled smart contract actually can be executed on certain blockchains, an additional step is required, namely, the payment of a transaction fee for the contract to be added to the chain and executed upon. In the case of the Ethereum blockchain, smart contracts are executed on the Ethereum Virtual Machine (EVM), and this payment, made through the ether cryptocurrency, is known as "gas." [1] The more complex the smart contract (based on the transaction steps to be performed), the more gas that must be paid to execute the smart contract. Thus, gas currently acts as an important gate to prevent overly complex or numerous smart contracts from overwhelming the EVM. [2]

CYBER2-29777 - 02141



Smart contracts are presently best suited to execute automatically two types of "transactions" found in many contracts: (1) ensuring the payment of funds upon certain triggering events and (2) imposing financial penalties if certain objective conditions are not satisfied. In each case, human intervention, including through a trusted escrow holder or even the judicial system, is not required once the smart contract has been deployed and is operational, thereby reducing the execution and enforcement costs of the contracting process.

As just one example, smart contracts could eliminate the so-called procure-to-pay gaps. When a product arrives and is scanned at a warehouse, a smart contract could immediately trigger requests for the required approvals and, once obtained, immediately transfer funds from the buyer to the seller. Sellers would get paid faster and no longer need to engage in dunning, and buyers would reduce their account payable costs. This could impact working capital requirements and simplify finance operations for both parties. On the enforcement side, a smart contract could be programmed to shut off access to an internet-connected asset if a payment is not received. For example, access to certain content might automatically be denied if payment was not received.

## Historical Background

The term "smart contract" was first introduced by computer scientist and cryptographer Nick Szabo some 20 years ago as a graduate student at University of Washington. According to Szabo:

New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart," because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises. [3]

Szabo's use of quotes around the word "smart" when comparing smart contracts to paper-based contracts, and his eschewing of artificial intelligence are important. Smart contracts may be "smarter" than paper contracts because they automatically can execute certain pre-programmed steps, but they should not be seen as intelligent tools that can parse a contract's more subjective requirements. Indeed, the classic example of a smart contract offered by Szabo is a vending machine. Once a purchaser has satisfied the conditions of the "contract" (i.e., inserting money into the machine) the machine automatically honors the terms of the unwritten agreement and delivers the snack.

Smart contracts today also find their origin in Ricardian Contracts, a concept published in 1996 by Ian Grigg and Gary Howland as part of their work on the Ricardo payment system to transfer assets. Grigg saw Ricardian Contracts as a bridge between text contracts and code that had the following parameters: a single document that "is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people (like a contract on paper), d) readable by programs (parsable like a database), e) digitally signed, f) carries the keys and server information, and g) allied with a unique and secure identifier." [4]

## The Interplay With Traditional Text Agreements

One of the difficulties with discussing smart contracts is that the term is used to capture two very different paradigms. The first involves smart contracts that are created and deployed without any enforceable text-based contract behind them. For example, two parties reach an oral understanding as to the business relationship they want to capture and then directly reduce that understanding into executable code. We refer to these below as "code-only smart contracts." The second paradigm involves the use of smart contracts as vehicles to effectuate certain provisions of a traditional text-based contract, in which the text itself references the use of the smart contract to effectuate certain provisions. We refer to these as "ancillary smart contracts."

## Are Smart Contracts Enforceable?

There is no federal contract law in the United States; rather, the enforceability and interpretation of contracts is determined at the state level. Thus, while certain core principles apply consistently across state lines, and there has been a drive to harmonize state laws by the National Conference of Commissioners on Uniform State Laws, any conclusions regarding smart contracts must be tempered by the reality that states may adopt different views.



A discussion regarding the enforceability of smart contracts must start with the fundamental distinction between an agreement and a "contract." States generally recognize that although two parties can enter into a variety of "agreements," a contract means that the agreement is legally binding and enforceable in a court of law. [5] In order to determine enforceability, state courts traditionally look to whether the common law requirements of offer, acceptance and consideration are satisfied. These basic requirements surely can be achieved through ancillary smart contracts. For example, an insurer might develop a flight insurance product that automatically provides the insured with a payout if a flight is delayed by more than two hours. [6] The key terms, such as delineating how the delay is calculated, can be set forth in a text-based contract, with the actual formation of the contract (payment of the premium) and the execution (automatic payout upon a verifiable delay) handled through an ancillary smart contract. Here, the insurer has made a definite offer for a flight insurance product that is accepted by the insured upon payment of the premium as consideration.

Although, today, certain contracts must be in writing, and additional formalities may be required such as those under the Uniform Commercial Code (UCC) and state statutes of frauds, [7] agreements do not always need to be in writing to be held enforceable. [8] Thus, many code-only smart contracts also will be enforceable under state laws governing contracts. Szabo's example of a vending machine is instructive in this regard. There, while the buyer has many implied rights, a contract was formed without any meaningful written terms other than a price display for each item. Thus, the fact that an agreement is rendered only in code, such as the case with code-only smart contracts, presents no particular barrier to contract formation outside the barriers imposed by the UCC and statutes of frauds. Indeed, a variety of laws and legal constructs have long considered the role of information technology in contract formation.

For example, the Uniform Electronic Transactions Act (UETA) which dates back to 1999 and forms the basis for state law in 47 states, provides that, with limited exceptions, electronic records, which include records created by computer programs, and electronic signatures (*i.e.*, digital signature using public key encryption technology) be given the same legal effect as their written counterparts. [9] UETA even goes so far as recognizing the validity of "electronic agents," which it defines as "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." [10] Under UETA, an electronic agent is "capable within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic agents once it has been activated by a party, without further attention of that party," [11] arguably a prescient acknowledgment of smart contracts.

Similarly, the federal Electronic Signatures Recording Act (E-Sign Act) not only recognizes the validity of electronic signatures and electronic records in interstate commerce, but also provides that a contract or other record relating to a transaction "may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound." [12] The term "electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response." [13]

Though an understanding of the current legal framework is important to evaluating the enforceability of smart contracts today, those using smart contracts in the future may not need to rely on laws that pre-date the development of blockchain technology. Arizona and Nevada already have amended their respective state versions of UETA to explicitly incorporate blockchains and smart contracts. [14] The fact that these states have adopted decidedly different definitions of those critical terms suggests that as more states follow their lead, there may be increasing pressure to adopt unified definitions to reflect blockchain and smart contract developments.

## Challenges With the Widespread Adoption of Smart Contracts

Given the existing legal frameworks for recognizing electronic contracts, it is quite likely that a court today would recognize the validity of code that executes provisions of a smart contract—what we have classified as ancillary smart contracts. There is also precedent to suggest that a code-only smart contract might enjoy similar legal protection. The challenge to widespread smart contract adoption may therefore have less to do with the limits of the law than with potential clashes between how smart contract code operates and how parties transact business. We set forth below certain of these challenges:



## How Can Non-technical Parties Negotiate, Draft and Adjudicate Smart Contracts?

A key challenge in the widespread adoption of smart contracts is that parties will need to rely on a trusted, technical expert to either capture the parties' agreement in code or confirm that code written by a third party is accurate. While some analogize this to hiring a lawyer to explain "the legalese" of a traditional text-based contract, the analogy is misplaced. Non-lawyers typically can understand simple short-form agreements as well as many provisions of longer agreements, especially those setting forth business terms. But a non-programmer would be at a total loss to understand even the most basic smart contract and is therefore significantly more beholden to an expert to explain what the contract "says."

To some extent, the inability of contracting parties to understand the smart contract code will not be a hindrance to entering into ancillary code agreements. This is because for many basic functions, text templates can be created and used to indicate what parameters need to be entered and how those parameters will be executed. For example, assume a simple smart contract function that extracts a late fee from a counterparty's wallet if a defined payment is not received by a specified date. The text template could prompt the parties to enter the amount of the expected payment, the due date and the amount of the late fee. However, a party may want to confirm that the underlying code actually will perform the functions specified in the text, and that there are no additional conditions or parameters—especially where the template disclaims any liability arising from the accuracy of the underlying code. This review will require a trusted third party with programming expertise.

In cases where such templates do not exist, and new code must be developed, the parties will need to communicate the intent of their agreement to a programmer. Simply handing that programmer a copy of the legal agreement would be inefficient since it would require the programmer to try and decipher a legal document. Parties relying on ancillary smart contracts therefore may need to draft a separate "term sheet" of functionality that the smart contract should perform and that can be provided to the programmer.

The parties also may want written representations from the programmer that the code performs as contemplated. The net result is that for customized arrangements that do not rely on an existing template, the parties may need to enter into a written agreement with the smart contract programmer, not unlike the contract that parties may enter into with a provider of services for Electronic Data Interchange (EDI) transactions today.

Insurance companies could also create policies to protect contracting parties from the risk that smart contract code does not perform the functions specified in the text of an agreement. Although the parties would also want to review (or have third parties review) the code, insurance can provide additional protection given that the parties might miss errors when reviewing the code. The parties would also take some additional comfort from the fact that the insurance company likely conducted its own code audit before agreeing to insure the code.

Code-only smart contracts used for business-to-consumer transactions could pose an additional set of issues that will need to be addressed. Courts are wary of enforcing agreements where the consumer did not receive adequate notice of the terms of the agreement, [15] and may be hesitant to enforce a smart contract where the consumer was not also provided with an underlying text agreement that included the complete terms.

Finally, as the validity or performance of smart contracts increasingly become adjudicated, courts may need a system of court-appointed experts to help them decipher the meaning and intent of the code. Today, parties routinely use their own experts when technical issues are at the center of a dispute. While both federal courts and many state courts have the authority to appoint their own experts, they rarely exercise that authority. [16] That approach may need to change if the number of standard contract disputes that center on interpreting smart contract code increases.

## Smart Contracts and the Reliance on "Off-chain" Resources

Many smart contract-proposed use-cases assume that the smart contract will receive information or parameters from resources that are not on the blockchain itself—so-called off-chain resources. For example, assume a crop insurance smart contract is programmed to transfer value to an insured party if the temperature falls below 32 degrees at any point. The smart contract will need to receive that temperature data from an agreed source. This presents two issues. First,



smart contracts do not have the ability to pull data from off-chain resources; rather, that information needs to be “pushed” to the smart contract. Second, if the data at issue is in constant flux, and since the code is replicated across multiple nodes across the network, different nodes may be receiving different information, even just a few seconds apart. In our example, Node-1 may receive information that the temperature is 31.9 degrees, while Node-2 may receive information that the temperature is actually 32 degrees. Given that consensus is required across the nodes for a transaction to be validated, such fluctuations can cause the condition to be deemed “not satisfied.”

Contracting parties will be able to solve this conundrum by using a so-called “oracle.” Oracles are trusted third parties that retrieve off-chain information and then push that information to the blockchain at predetermined times. In the foregoing example, the oracle would monitor the daily temperature, determine that the freezing event has occurred and then push that information to the smart contract.

Although oracles present an elegant solution to accessing off-chain resources, this process adds another party with whom the parties would need to contract to effectuate a smart contract, thus somewhat diluting the decentralized benefits of smart contracts. It also introduces a potential “point of failure.” For example, an oracle might experience a system flaw and be unable to push out the necessary information, provide erroneous data or simply go out of business. Smart contracts will need to account for these eventualities before their adoption can become more widespread.

### **What is the “Final” Agreement Between the Parties?**

When analyzing traditional text-based contracts, courts will examine the final, written document to which the parties have agreed in order to determine whether the parties are in compliance or breach. Courts have long emphasized that it is this final agreement that represents the mutual intent of the parties—the “meeting of the minds.”

In the case of code-only smart contracts, the code that is executed—and the outcome it produces—represents the only objective evidence of the terms agreed to by the parties. In these cases, email exchanges between the parties as to what functions the smart contract “should” execute, or oral discussions to that effect, likely would yield to the definitive code lines as the determinative manifestation of the parties’ intent.

With respect to ancillary smart contracts, a court likely would look at the text and code as a unified single agreement. The issue becomes complicated when the traditional text agreement and the code do not align. In the crop insurance example described above, assume the text of an agreement specifies that an insurance payout will be made if the temperature falls below 32 degrees, while the smart contract code triggers the payment if the temperature is equal to or below 32 degrees. Assuming that the text agreement does not state whether the text or code controls in the event of an inconsistency, courts will need to determine—perhaps on a case-by-case basis—whether the code should be treated as a mutually agreed amendment to the written agreement or whether the text of the agreement should prevail. In some respects, the analysis should be no different than a case where the provisions of a main agreement differ from what is reflected in an attached schedule or exhibit. The fact that here the conflict would be between text and computer code and not two text documents should not be determinative, but courts may take a different view.

One solution will be for parties to use a text based contract where the parameters that trigger the smart contract execution are not only visible in the text but actually populate the smart contract. In our example, “less than 32 degrees” would not only be seen in the text, but also would create the parameter in the smart contract itself, thereby minimizing the chances of any inconsistency.

### **The Automated Nature of Smart Contracts**

One of the key attributes of smart contracts is their ability to automatically and relentlessly execute transactions without the need for human intervention. However, this automation, and the fact that smart contracts cannot easily be amended or terminated unless the parties incorporate such capabilities during the creation of the smart contract, present some of the greatest challenges facing widespread adoption of smart contracts.

For example, with traditional text contracts, a party can easily excuse a breach simply by not enforcing the available penalties. If a valued customer is late with its payment one month, the vendor can make a real-time decision that



preserving the long-term commercial relationship is more important than any available termination right or late fee. However, if this relationship had been reduced to a smart contract, the option not to enforce the agreement on an *ad hoc* basis likely would not exist. A late payment will result in the automatic extraction of a late fee from the customer's account or the suspension of a customer's access to a software program or an internet-connected device if that is what the smart contract was programmed to do. The automated execution provided by smart contracts might therefore not align with the manner in which many businesses operate in the real world.

Similarly, in a text-based contractual relationship, a party may be willing to accept, on an *ad hoc* basis, partial performance to be deemed full performance. This might be because of an interest in preserving a long-term relationship or because a party determines that partial performance is preferable to no performance at all. Here, again, the objectivity required for smart contract code might not reflect the realities of how contracting parties interact.

## Amending and Terminating Smart Contracts

At present, there is no simple path to amend a smart contract, creating certain challenges for contracting parties. For example, in a traditional text-based contract, if the parties have mutually agreed to change the parameters of their business deal, or if there is a change in law, the parties quickly can draft an amendment to address that change, or simply alter their course of conduct. Smart contracts currently do not offer such flexibility. Indeed, given that blockchains are immutable, modifying a smart contract is far more complicated than modifying standard software code that does not reside on a blockchain. The result is that amending a smart contract may yield higher transaction costs than amending a text-based contract, and increases the margin of error that the parties will not accurately reflect the modifications they want to make.

Similar challenges exist with respect to terminating a smart contract. Assume a party discovers an error in an agreement that gives the counterparty more rights than intended, or concludes that fulfilling its stated obligations will be far more costly than it had expected. In a text-based contract, a party can engage in, or threaten, so-called "efficient breach," *i.e.*, knowingly breaching a contract and paying the resulting damages if it determines that the cost to perform is greater than the damages it would owe. Moreover, by ceasing performance, or threatening to take that step, a party may bring the counterparty back to the table to negotiate an amicable resolution. Smart contracts do not yet offer analogous self-help remedies.

Projects are currently underway to create smart contracts that are terminable at any time and more easily amended. While in some ways this is antithetical to the immutable and automated nature of smart contracts, it reflects the fact that smart contracts only will gain commercial acceptance if they reflect the business reality of how contracting parties act.

## Objectivity and the Limits of Incorporating Desired Ambiguity Into Smart Contracts

The objectivity and automation required of smart contracts can run contrary to how business parties actually negotiate agreements. During the course of negotiations, parties implicitly engage in a cost-benefit analysis, knowing that at some point there are diminishing returns in trying to think of, and address, every conceivable eventuality. These parties no longer may want to expend management time or legal fees on the negotiations, or may conclude that commencing revenue generating activity under an executed contract outweighs addressing unresolved issues. Instead, they may determine that if an unanticipated event actually occurs, they will figure out a resolution at that time. Similarly, parties may purposefully opt to leave a provision somewhat ambiguous in an agreement in order to give themselves the flexibility to argue that the provision should be interpreted in their favor. This approach to contracting is rendered more difficult with smart contracts where computer code demands an exactitude not found in the negotiation of text-based contracts. A smart contract cannot include ambiguous terms nor can certain potential scenarios be left unaddressed. As a result, parties to smart contracts may find that the transaction costs of negotiating complex smart contracts exceed that of a traditional text-based contracts.

It will take some time for those adopting smart contracts in a particular industry to determine which provisions are sufficiently objective to lend themselves to smart contract execution. As noted, to date, most smart contracts perform relatively simple tasks where the parameters of the "if/then" statements are clear. As smart contracts increase in



complexity, parties may disagree on whether a particular contractual provision can be captured through the objectivity that a smart contract demands.

## Do Smart Contracts Really Guarantee Payment?

One benefit often touted of smart contracts is that they can automate payment without the need for dunning notices or other collection expenses and without the need to go to court to obtain a judgment mandating payment. While this is indeed true for simpler use cases, it may be less accurate in complex commercial relationships. The reality is that parties are constantly moving funds throughout their organization and do not “park” total amounts that are due on a long-term contract in anticipation of future payment requirements. Similarly, a person obtaining a loan is unlikely to keep the full loan amount in a specified wallet linked to the smart contract. Rather, the borrower will put those funds to use, funding the necessary repayments on an *ad hoc* basis.

If the party owing amounts under the smart contract fails to fund the wallet on a timely basis, a smart contract looking to transfer money from that wallet upon a trigger event may find that the requisite funds are not available. Implementing another layer into the process, such as having the smart contract seek to pull funds from other wallets or having that wallet “fund itself” from other sources, would not solve the problem if those wallets or sources of funds also lack the requisite payment amounts. The parties might seek to address this issue through a text-based requirement that a wallet linked to the smart contract always have a minimum amount, but that solution simply would give the party a stronger legal argument if the dispute was adjudicated. It would not render the payment operation of the smart contract wholly automatic. Thus, although smart contracts will render payments far more efficient, they may not eliminate the need to adjudicate payment disputes.

## Risk Allocation for Attacks and Failures

Smart contracts introduce an additional risk that does not exist in most text-based contractual relationships—the possibility that the contract will be hacked or that the code or protocol simply contains an unintended programming error. Given the relative security of blockchains, these concepts are closely aligned; namely, most “hacks” associated with blockchain technology are really exploitations of an unintended coding error. As with many bugs in computer code, these errors are not glaring, but rather become obvious only once they have been exploited. For example, in 2017 an attacker was able to drain several multi-signature wallets offered by Parity of \$31 million in ether. [17] Multi-signature wallets add a layer of security because they require more than one private key to access the wallet. However, in the Parity attack, the attacker was able to exploit a flaw in the Parity code by reinitializing the smart contract and making himself or herself the sole owner of the multi-signature wallets. Parties to a smart contract will need to consider how risk and liability for unintended coding errors and resulting exploitations are allocated between the parties, and possibly with any third party developers or insurers of the smart contract.

## Governing Law and Venue

One of the key promises of blockchain technology, and by extension smart contracts, is the development of robust, decentralized and global platforms. However, global adoption means that parties may be using a smart contract across far more jurisdictions than might exist in the case of text-based contracts. The party offering terms under a smart contract would therefore be best-served by specifying the governing law and venue for that smart contract. A governing law provision specifies what substantive law will apply to the interpretation of the smart contract, whereas a venue clause specifies which jurisdiction's courts will adjudicate the dispute. In cases where governing law or venue is not specified, a plaintiff may be relatively unconstrained in choosing where to file a claim or in arguing which substantive law should apply given the wide range of jurisdictions in which a smart contract might be used. Given that many early disputes concerning smart contracts will be ones of first-impression, contracting parties will want some certainty surrounding where such disputes will be adjudicated.

## Best Practices

Given that we are at the nascent stages of smart contract adoption, best practices for implementing such code is still evolving. However, the checklist below should help developers design effective smart contracts and guide companies who



plan to use them.

- For now, parties entering into any type of contractual arrangement would be best served using a hybrid approach that combines text and code. As noted, there are strong arguments that code-only smart contracts should be enforceable, at least under state contract law in the U.S. However, until there is greater clarity on their validity and enforceability, code-only smart contracts should be used only for simpler transactions. Parties will continue to want text-versions of agreements so they can read the agreed-upon terms, memorialize terms that smart contracts are not equipped to address and have a document they know a court will enforce.
- In a hybrid contract using text and code, the text should clearly specify the smart contract code with which it is associated, and the parties should have full visibility into the variables that are being passed to the smart contract, how they are defined and the transaction events that will trigger execution of the code.
- When relying on oracles for off-chain data, the parties should address what would happen if the oracle is unable to push out the necessary data, provides erroneous data or simply goes out of business.
- The parties should consider risk allocation in the event of a coding error.
- The text agreement accompanying the code should specify the governing law and venue, as well as the order of precedence between text and code in the event of a conflict.
- The text agreement should include a representation by each party that they have reviewed the smart contract code, and that it reflects the terms found in the text agreement. Although such a representation cannot force a party to examine the code, it will help the counterparty defend against a claim that the code was never reviewed. Parties may also choose to insure against the risk that the code contains errors. As noted, parties may need to involve third-party experts to review the code.

## Future of Smart Contracts

Today, smart contracts are a prototypical example of "Amara's Law," the concept articulated by Stanford University computer scientist Roy Amara that we tend to overestimate new technology in the short run and underestimate it in the long run. Although smart contracts will need to evolve before they are widely adopted for production use in complex commercial relationships, they have the impact to revolutionize the reward and incentive structure that shapes how parties contract in the future. To that end, and when thinking about smart contracts, it is important not to simply think how existing concepts and structures can be ported over to this new technology. Rather, the true revolution of smart contracts will come from entirely new paradigms that we have not yet envisioned.

## Endnotes

<sup>1</sup> See "What is the 'Gas' in Ethereum?" *Cryptocompare*, November 18, 2016, [available here](#).  
([go back](#))

<sup>2</sup> *Id.*  
([go back](#))

<sup>3</sup> Nick Szabo, "Smart Contracts: Building Blocks for Digital Market," 1996, [available here](#).  
([go back](#))

<sup>4</sup> Ian Grigg, "The Ricardian Contract," [available here](#).  
([go back](#))

<sup>5</sup> See, e.g., "Restatement (Second) of Contracts," Section 1, American Law Institute, 1981. In the U.S., contract law is ordinarily a function of state law. Although this article outlines general contract law principles that are common across states, we note that state law differences may impact the enforceability of smart contracts in certain states.



[\(go back\)](#)

<sup>6</sup> At least one company, AXA, currently offers such a product. [See here](#).

[\(go back\)](#)

<sup>7</sup> See, e.g., UCC § 2-201.

[\(go back\)](#)

<sup>8</sup> See, e.g., *Lumhoo v. Home Depot USA, Inc.*, 229 F. Supp. 2d 121, 160 (E.D.N.Y. 2002) (holding that the plaintiffs adduced sufficient evidence to support an inference that the parties formed an oral contract for payment by their employer at an overtime rate for any hours worked in excess of eight hours per day).

[\(go back\)](#)

<sup>9</sup> Uniform Electronic Transactions Act (Unif. Law Comm'n 1999)—New York, Illinois and Washington have state-specific laws relating to the validity of electronic transactions.

[\(go back\)](#)

<sup>10</sup> *Id.* § 2(6).

[\(go back\)](#)

<sup>11</sup> *Id.* § 2 cmt. 5.

[\(go back\)](#)

<sup>12</sup> 15 U.S.C. § 7001(h).

[\(go back\)](#)

<sup>13</sup> 15 U.S.C. § 7006(3).

[\(go back\)](#)

<sup>14</sup> See 2017 Ariz. HB 2417 44-7061 and Nev. Rev. Stat. Ann. § 719.090.

[\(go back\)](#)

<sup>15</sup> See, e.g., *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220 (2d Cir. 2016) (reversing the district court's dismissal for failure to state a claim and holding that reasonable minds could disagree as to whether Amazon provided the consumer with reasonable notice of the mandatory arbitration provision at issue).

[\(go back\)](#)

<sup>16</sup> See Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure*, Section 6304 (3d ed. supp. 2011) ("In fact, the exercise of Rule 706 powers is rare under virtually any circumstances. This is, at least in part, owing to the fact that appointing an expert witness increases the burdens of the judge, increases the costs to the parties, and interferes with the adversarial control over the presentation of evidence."), and Stephanie Domitrovich, Mara L. Merino & James T. Richardson, *State Trial Judge Use of Court Appointed Experts: Survey Results and Comparisons*, 50 *Jurimetrics J.* 371, 373–74 (2010).

[\(go back\)](#)

<sup>17</sup> See Haseeb Qureshi, "A Hacker Stole \$31M of Ether—How it Happened, and What it Means for Ethereum," *FreeCodeCamp*, (July 20, 2017), [available here](#).

[\(go back\)](#)

---

Both comments and trackbacks are currently closed.

**TAB 74**



**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF FLORIDA  
PENSACOLA DIVISION**

**COIN CENTER, et al.,**

**Plaintiffs,**

**v.**

**Case No. 3:22cv20375-TKW-ZCB**

**JANET YELLEN, in her Official  
Capacity as Secretary of the Treasury,  
et al.,**

**Defendants.**

---

**ORDER ON CROSS-MOTIONS FOR SUMMARY JUDGMENT**

This case is before the Court based on the parties' cross-motions for summary judgment (Docs. 36, 57). Upon due consideration of the motions, Plaintiffs' supporting memorandum (Doc. 36-1), the responses (Docs. 57, 62), the replies (Docs. 62, 66), the amicus briefs (Docs. 42-1, 45-1, 46-1, 60-1), the joint appendix of administrative record documents (Doc. 67), the classified lodging (*see* Doc. 69),<sup>1</sup> and Defendants' notice of supplemental authority (Doc. 70) and Plaintiffs' response (Doc. 71), the Court finds that Defendants' motion is due to be granted and Plaintiffs' motion is due to be denied.

---

<sup>1</sup> The Court reviewed the classified lodging *in camera*.

## **Regulatory Background**

The International Emergency Economic Powers Act (IEEPA) authorizes the President to declare national emergencies “to deal with any unusual and extraordinary [foreign] threat ... to the national security, foreign policy, or economy of the United States.” 50 U.S.C. §1701(a). Pursuant to that authority, the President declared national emergencies with respect to malicious foreign cyber-enabled activities, *see* Exec. Order No. 13694 (Apr. 1, 2015), as amended by Exec. Order No. 13757 (Dec. 28, 2016), and North Korea’s pursuit of its nuclear missile program, *see* Exec. Order No. 13722 (Mar. 15, 2016).

After a national emergency is declared, the IEEPA authorizes the President to “regulate ... or prohibit ... any use [of], transfer [of], ... dealing in, ... or transactions involving, any property in which any foreign country or a national thereof has any interest.” 50 U.S.C. §1702(a)(1)(B). Pursuant to that authority, the President blocked all property and interests in property of any person determined by the Secretary of the Treasury to have materially assisted, sponsored, or provided financial, material, or technological support for foreign malicious cyber-enabled activities that threaten the national security, foreign policy, or economic health or financial stability of the United States, *see* Exec. Order Nos. 13694, 13757, and the North Korean government, *see* Exec. Order No. 13722.



The Secretary of the Treasury delegated the authority granted by Executive Orders 13694 and 13722 to the Director of the Office of Financial Assets Control (OFAC). *See* 31 C.F.R. §§510.802, 578.802.

On November 8, 2022,<sup>2</sup> OFAC designated “Tornado Cash” as a Specially Designated National or Blocked Person. *See* A.R. 1. The effect of the designation is that “unless licensed or otherwise authorized by [OFAC], (1) all real, personal, and any other property and interests in property of [Tornado Cash] ... are blocked and may not be transferred, paid, exported, withdrawn or otherwise dealt in, and (2) any transaction or dealing ... in property or interests in property of [Tornado Cash] is prohibited.” A.R. 4.

The designation described Tornado Cash as

an entity with an organizational structure that consists of: (1) its founders—Alexey Pertsev, Roman Semenov, and Roman Storm—and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado Cash Decentralized Autonomous Organization (DAO), and actively promote the platform’s popularity in an attempt to increase its user base; and (2) the Tornado Cash DAO, which is responsible for voting on and implementing those new features created by the developers.

A.R. 1. The designation listed 91 Internet addresses that were affiliated with Tornado Cash, including the addresses for the “smart contracts” that Plaintiffs refer

---

<sup>2</sup> Tornado Cash was initially designated by OFAC on August 8, 2022, but that designation was “wholly replaced” by the November 8 “redesignat[ion].” *See* A.R. 10.

to as the “core software tool” of the Tornado Cash service.<sup>3</sup> A.R. 1-4.

The designation was based on a 66-page “evidentiary memorandum” that detailed how Tornado Cash worked, A.R. 33-64, and how it had been used to facilitate malicious cyber-enabled activities by laundering hundreds of millions of dollars of cryptocurrency stolen by groups sponsored by North Korea, including the Lazarus Group, A.R. 67-78. The memorandum was supported by 229 exhibits that contained over 2,400 pages. A.R. 79-100; *see also* Doc. 19-2 (index of the entire administrative record).

Along with the designation, OFAC published several Frequently Asked Questions (FAQs) on its website to inform the public about the scope of the designation. *See* OFAC, *Frequently Asked Questions: Cyber-Related Sanctions*, <https://perma.cc/5KQ5-25GE>.<sup>4</sup> For example, FAQ 1079 explained that individuals who had funds held in Tornado Cash at the time of designation may request a specific license for retrieval of the funds and that “OFAC would have a favorable licensing policy towards such applications, provided that the transaction did not involve other

---

<sup>3</sup> According to Plaintiffs, the “core software tool” consists of under 500 lines of computer code that is published to 20 of the addresses listed in the designation. *See* Doc. 36-1 at 12. The code at each address is identical, except that each address is designed for a different amount and/or type of crypto assets. *Id.* at 12-13.

<sup>4</sup> The FAQs are not included in the administrative record, but they were specifically referenced in the press release announcing the re-designation of Tornado Cash that is included in administrative record. *See* A.R. 12 (“For additional information and guidance regarding sanctions implications specific to Tornado Cash, please reference OFAC’s **FAQs 1076-1079** and **FAQ 1095**.”) (bold language is hyperlinked in original).



sanctionable conduct.” Similarly, FAQ 1078 explained that although unsolicited receipt of crypto assets from Tornado Cash (i.e., “dusting”) would technically be subject to OFAC’s regulations, OFAC will not prioritize enforcement against persons who receive such funds.

### **Technical Background**

Cryptocurrency is a virtual currency that can be used for payment or investment purposes. A.R. 21, 1766–67. It is traded and exchanged on a “blockchain,” which is a decentralized ledger that relies on an online network of individuals to maintain the ledger’s accuracy through the use of cryptographic algorithms. A.R. 21, 875.

Cryptocurrency can take the form of virtual coins or tokens. A.R. 22, 729–31. Coins are the mediums of exchange on a blockchain and are akin to dollars and cents. A.R. 22, 731. Tokens are assets created through software developed on a blockchain that can be used for a particular purpose, but they also have value and can be bought, sold, and traded on secondary markets. *Id.*

A governance token is a specific type of token that can represent a share of ownership or voting rights in the mixing service’s decentralized autonomous organization (DAO). *Id.* The DAO is an entity composed of the holders of governance tokens who manage the service by voting on organizational decisions.

A.R. 24, 515. Normally, the core developer group creates the DAO and distributes governance tokens to stakeholders. A.R. 515.

Ethereum is a popular cryptocurrency blockchain and its native coin is Ether (ETH). A.R. 26, 818, 857–58. An Ethereum account is a “wallet” that can hold and send ETH along the Ethereum blockchain. A.R. 506.

When a user makes a transaction using Ethereum, the transaction is posted to a public ledger visible to anyone. A.R. 17. The public ledger displays the sender’s wallet address, the recipient’s wallet address, and the crypto asset that they exchanged. A.R. 23. Thus, anyone can view every Ethereum transaction ever made on the public ledger and can trace an individual’s transaction history. A.R. 549.

Tornado Cash is a cryptocurrency “mixing service” that was founded by two Russians (Alexey Pertsev and Roman Semenov), Roman Storm, and other associated developers. A.R. 32. Those individuals launched the service, developed new features, created the DAO, and actively promoted the platform’s popularity. *Id.*

Tornado Cash’s DAO is made up of users who hold TORN, which is Tornado Cash’s governance token. A.R. 35–41. Tornado Cash’s founders also hold TORN. A.R. 32, 35–41. The founders and DAO include foreigners. *Id.*

TORN holders have the right to vote on any changes to the Tornado Cash software. A.R. 35–41. TORN holders also have an interest in the increased use and popularity of the Tornado Cash service because TORN is a virtual asset that can be



bought and sold on secondary markets and its value has the potential to increase as the popularity of the service increases. A.R. 43–50.

The Tornado Cash service uses smart contracts—which are essentially computer software created by its developers and approved and deployed by the DAO on the Ethereum blockchain. A.R. 51; *see also* A.R. 818, 820, 2141. The smart contracts allow Ethereum users to deposit ETH into a “pool” where it is mixed with other users’ deposits and then withdrawn at a time of the user’s choosing. A.R. 51. The more users that have deposited ETH into the pool the more difficult it is to connect the withdrawal with a particular deposit, which thereby provides a degree of anonymity to the user’s transaction that is not available on the public ledger. A.R. 16–17.

The smart contracts that make up what Plaintiffs refer to as Tornado Cash’s “core software tool” are immutable in that they cannot be changed by anyone, including the developers and the DAO. A.R. 563-67, 951.

Tornado Cash transactions can be (and 84% are) executed with the aid of third-party “relayers.” A.R. 57 n.113. The use of a relayer makes it even harder to identify the parties to the transaction, but transactions can be completed without a relayer. A.R. 57, 187.

If a registered relayer is used, the depositor pays a fee to the relayer and the relayer pays a portion of that fee to members of the Tornado Cash DAO in the form

of TORN. A.R. 57. If a registered relayer is not used, no fee is paid to the DAO. A.R. 56–60.

TORN had value before the option of using relayers was added to the Tornado Cash service in March 2022, but the value of TORN increased significantly after relayers were added. A.R. 38-39, 1596. TORN continued to have value after OFAC’s initial designation of Tornado Cash, albeit considerably less than it had before the designation. A.R. 152-53.

### **Procedural Background**

OFAC’s designation of Tornado Cash was challenged by Plaintiffs<sup>5</sup> in this case and by other plaintiffs in a case in the Western District of Texas. The issues raised in the two cases are similar, but not identical.

In August 2023, the judge in the Western District of Texas case granted summary judgment in favor of the Government. *See Van Loon v. Dep’t of Treasury*, 2023 WL 5313091 (W.D. Tex. Aug. 17, 2023) (Pitman, J.), *appeal filed*, No. 23-50669 (5th Cir. Sep. 18, 2023). The court found that Tornado Cash is an “entity” that may be designated under the IEEPA and Executive Orders 13694 and 13722 and that Tornado Cash has a property interest in the smart contracts listed in the

---

<sup>5</sup> Plaintiffs are three individuals who use Tornado Cash for various purposes (including making donations to organizations and causes they support) and a nonprofit cryptocurrency advocacy organization that regularly receives donations from individuals through Tornado Cash.



designation. *Id.* at \*11. The court also rejected the plaintiffs’ constitutional claims under the First Amendment and Takings Clause. *Id.* at \*12.

In this case, Plaintiffs do not challenge OFAC’s determination that Tornado Cash is a foreign entity that can be designated, *see* Doc. 36-1 at 34,<sup>6</sup> and they only challenge the designation as it relates to 29 of the 91 addresses<sup>7</sup> affiliated with Tornado Cash because they contend that those addresses are not property in which a foreigner has “any interest.”

Plaintiffs claim that the designation of Tornado Cash’s core software tool should be held unlawful and set aside under the Administrative Procedure Act (APA) because the designation (1) exceeded OFAC’s statutory authority and was contrary to law, (2) was arbitrary and capricious, and (3) violated their rights of association under the First Amendment. Defendants<sup>8</sup> responds that the designation of Tornado

---

<sup>6</sup> Several of the amici make this argument, but the Court declines to consider it because “a district court should not consider arguments raised by amici that go beyond the issues properly raised by the parties.” *Victim Rights Law Ctr. v. Rosenfelt*, 988 F.3d 556, 564 n.8 (1st Cir. 2021), *cert. denied sub nom. Found. for Individual Rights in Educ. v. Victim Rights Law Ctr.*, 142 S. Ct. 754 (2022); *see also F.T.C. v. Phoebe Putney Health Sys., Inc.*, 568 U.S. 216, 226 n.4 (2013) (declining to consider issues raised by amici that were not raised by the parties or addressed by the lower courts); *New Jersey v. New York*, 523 U.S. 767, 781 n.3 (1998) (same).

<sup>7</sup> Plaintiffs are only challenging the designation of the 20 “core software tool” addresses and 9 additional addresses “that host ancillary tools that cannot be controlled or changed by anybody.” Doc. 36-1 at 14-15. Plaintiffs are not challenging the other 62 addresses listed in the designation. *Id.* at 15.

<sup>8</sup> Defendants are Janet Yellen, in her official capacity as Secretary of the Treasury; the Department of the Treasury; Andrea Gacki, in her official capacity as Director of OFAC; and OFAC.

Cash in its entirety was within OFAC’s statutory authority, was not arbitrary and capricious, and did not violate the First Amendment.

There is no dispute that Plaintiffs have standing to challenge the designation because it will prohibit them from using Tornado Cash in the future. Thus, the case can be resolved on the merits.

There are no factual issues in dispute, so the Court need only decide based on a review of the administrative record and the parties’ cross-motions for summary judgment which party is entitled to judgment as a matter of law. *See* Fed. R. Civ. P. 56(a) (“The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.”). The motions were extensively<sup>9</sup> briefed and are ripe for rulings. No hearing is needed to rule on the motions.<sup>10</sup>

### **Standard of Review**

Under the APA, the Court has the authority to “hold unlawful and set aside” agency action that is “arbitrary [or] capricious,” 5 U.S.C. §706(2)(A), “contrary to [a] constitutional right,” *id.* at §706(2)(B), or “in excess of statutory jurisdiction, authority, or limitations,” *id.* at §706(2)(C). The standard of review under the APA

---

<sup>9</sup> The parties filed 180 pages of briefs, and an additional 146 pages of amicus briefs were filed.

<sup>10</sup> Plaintiffs requested oral argument, *see* Doc. 36 at 2, but the Court sees no need for it based on the extensive briefing. *See* N.D. Fla. Loc. R. 7.1(K) (“The Court may—and most often does—rule on a motion without oral argument, even if a party requests oral argument.”).



is “exceedingly deferential” to the agency, *see Sierra Club v. Van Antwerp*, 526 F.3d 1353, 1360 (11th Cir. 2008) (quoting *Fund for Animals, Inc. v. Rice*, 85 F.3d 535, 541 (11th Cir. 1996)), particularly on matters involving foreign policy, *see Dames & Moore v. Regan*, 453 U.S. 654, 672 (1981) (explaining that “the legislative history and cases interpreting [the statute on which the IEEPA was patterned] fully sustain the broad authority of the Executive”) *Zarmach Oil Services, Inc. v. U.S. Dept. of the Treasury*, 750 F. Supp. 2d 150, 155 (D.D.C. 2010) (“[C]ourts owe a substantial measure of ‘deference to the political branches in matters of foreign policy,’ including cases involving blocking orders.”)(quoting *Regan v. Wald*, 468 U.S. 222, 242 (1984)); *Holy Land Found. for Relief & Dev. v. Ashcroft*, 219 F. Supp.2d 57, 84 (D.D.C. 2002) (“Blocking orders are an important component of U.S. foreign policy, and the President's choice of this tool to combat terrorism is entitled to particular deference.”), *aff'd*, 333 F.3d 156 (D.C. Cir. 2003).

In determining whether agency action is arbitrary or capricious, the Court’s role is to ensure that the agency’s decision was rational, “not to conduct its own investigation and substitute its own judgment for the administrative agency’s decision.” *Sierra Club*, 526 F.3d at 1360 (quoting *Pres. Endangered Areas of Cobb’s Hist., Inc. v. U.S. Army Corps of Eng’rs*, 87 F.3d 1242, 1246 (11th Cir. 1996)). However, the Court is not required to defer to the agency’s interpretation of unambiguous statutory or regulatory language. *See Kinsor v. Wilkie*, 139 S.Ct. 2400,

2415-18 (2019); *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 457 U.S. 837, 842-43 (1984).

### **Analysis**

The parties’ filings frame three issues—(1) whether OFAC exceed its statutory authority by designating Tornado Cash’s core software tool; (2) whether the designation was arbitrary or capricious; and (3) whether the designation violated the First Amendment. Each issue will be addressed in turn.

#### Statutory Authority

Plaintiffs argue that OFAC exceeded its statutory authority in designating Tornado Cash’s core software tool because the tool is merely computer code that cannot be changed by anyone and in which no foreigner has a legally recognized “property interest.” The Court rejects this argument because it is built on the faulty premise that the “interest” required under the IEEPA is “property interest” or “ownership interest” in the technical legal sense.

The operative language in the IEEPA is “any interest,” not “property interest” or “ownership interest.” This statutory language has been interpreted broadly by the other courts. *See Holy Land*, 219 F. Supp. 2d at 67 (explaining that the IEEPA “does not limit the President’s blocking authority to the existence of a legally enforceable interest”); *OKKO Bus. PE v. Lew*, 133 F. Supp. 3d 17, 23–24 (D.D.C. 2015) (“The sweeping language of [50 U.S.C. §]1702 imposes no limit on the scope of interest



blockable under the IEEPA.”) (quoting *Holy Land*, 333 F.3d at 162); *Global Relief Found., Inc. v. O’Neill*, 315 F.3d 748, 753 (7th Cir. 2002) (“The function of the IEEPA strongly suggests that beneficial rather than legal interests matter.”). And the broad interpretation of the phrase “any interest” is consistent with its plain language because the word “any” is “used to indicate one selected without restriction,” Webster’s Seventh Collegiate Dictionary, at 40 (1965), and the word “interest” is a general word that is “to be accorded [its] full and fair scope [and is] not to be arbitrarily limited,” Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 101 (2012).

The regulations adopted by OFAC define the term “interest” when used with respect to property to mean “an interest of any nature whatsoever, direct or indirect.” 31 C.F.R. §§510.313, 578.309. This definition is consistent with the broad, plain-language interpretation of the phrase “any interest” and, thus, the regulations are entitled to deference. *See Consarc Corp. v. Iraqi Ministry*, 27 F.3d 695, 701 (D.C. Cir. 1994) (“OFAC may choose and apply its own definition of property interest, subject to deferential judicial review.”); *OKKO*, 133 F. Supp. 3d at 25 (explaining that the OFAC’s interpretation of the definition of “interest” in its regulations is entitled to deference unless “OFAC’s construction has departed so far from common usage as to be ‘plainly wrong.’”).

Based on OFAC's regulations, the question as to whether OFAC has exceeded its delegated authority by designating the Tornado Cash core software tool boils down to whether members of the Tornado Cash entity (i.e., its founders, developers, and DAO) have "an interest of any nature whatsoever" in that tool. On that issue, the administrative record establishes that the Tornado Cash entity has an "interest" in all of the smart contracts that make up its service (including the core software tool) because without those contracts, the service and the TORN held by the founders, developers, and DAO would not function and would be less valuable. *See, e.g.,* A.R. 60-62.

The Court did not overlook Plaintiffs' argument that the Tornado Cash entity has "abandoned" any interest it may have had in the core software tool because the "tool [is now] inalterable and irrevocable." Doc. 36-1 at 22. However, as persuasively explained in the evidentiary memorandum, TORN holders still have an indirect beneficial "interest" in the use of the core software tool and the service as a whole because that increases the value of the TORN. *See* A.R. 61 (explaining that "TORN owners and the DAO are ... similar to stockholders, who have an interest in the enterprise, and may benefit from the success of TORNADO CASH [because] the more users that submit virtual currency to the smart contracts to be mixed, the larger the pool becomes, and the more effective the virtual currency may be mixed, thereby increasing the value of TORNADO CASH and of TORN tokens").



The Court also did not overlook that the core software tool does not directly generate fees for TORN holders when the tool is used without the involvement of a registered relayer. However, the indirect interest that TORN holders (including the Tornado Cash founders, developers, and DAO) have in the increased use and popularity of the Tornado Cash service as a whole is sufficient to establish that foreigners have an “interest” in the core software tool. Indeed, the fact that TORN had substantial value before relayers (and the fees they paid) were added to the Tornado Cash service in March 2022 suggests that the service has intrinsic value even without relayers and supports the inference that increased use of the service will increase the value of the TORN held by Tornado Cash’s founders, developers, and DAO—which is an “interest” for purposes of the IEEPA.

Finally, the Court did not overlook the statement in *Regan* that “[t]he grant of authorities in IEEPA does not include the power ... to regulate purely domestic transactions.” 468 U.S. at 228 n.8. However, that does not help Plaintiffs because a Tornado Cash transaction between two Americans cannot be considered a “purely domestic transaction” when the transaction provides indirect benefits to foreigners by increasing the value of the TORN held by the Tornado Cash founders, developers, and DAO.

In sum, because foreigners (e.g., Tornado Cash’s founders, developers, and DAO) have a financial “interest” in the increased use and popularity of the Tornado

Cash service as a whole, OFAC did not exceed its statutory authority by designating all of the addresses affiliated with the service, including the core software tool, under the IEEPA. This conclusion is not undercut by the rule of lenity or the major questions doctrine.

The rule of lenity is a canon of statutory interpretation that requires courts to construe any ambiguity in a statute defining a crime or imposing a penalty in favor of the defendant. *See* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 296 (2012). The rule of lenity could be implicated here because, even though this is not a criminal case, the IEEPA imposes criminal penalties, *see* 50 U.S.C. §1705(a), (c), and “when [courts] are faced with a statute that has both criminal and noncriminal applications, ‘[they] must interpret the statute consistently’ in both contexts.” *Romero v. Sec’y, U.S. Dep’t of Homeland Sec.*, 20 F.4th 1374, 1383 (11th Cir. 2021), *cert. denied sub nom. Argueta Romero v. Mayorkas*, 142 S. Ct. 2869 (2022) (quoting *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004)). However, “[t]he rule [of lenity] ‘applies only when, after consulting traditional canons of statutory construction, we are left with an ambiguous statute.’” *Moskal v. United States*, 498 U.S. 103, 108 (1990); *see also Shular v. United States*, 140 S. Ct. 779, 787 (2020) (quoting *United States v. Shabani*, 513 U.S. 10, 17



(1994)). Here, as discussed above, there is nothing ambiguous about the statutory phrase “any interest” that would justify invocation of the rule of lenity.<sup>11</sup>

The major questions doctrine “refers to an identifiable body of law that has developed over a series of significant cases all addressing a particular and recurring problem: agencies asserting highly consequential power beyond what Congress could reasonably be understood to have granted.” *W. Virginia v. Env’tl. Prot. Agency*, 142 S. Ct. 2587, 2609 (2022). Accordingly, “in certain extraordinary cases ... [t]he agency ... must point to ‘clear congressional authorization’ for the power it claims.” *Id.* (emphasis added) (quoting *Util. Air Regulatory Group v. E.P.A.*, 573 U.S. 302, 324 (2014)). This is based on the logic that “had Congress wished to assign th[ose] question[s] to an agency, it surely would have done so expressly.” *King v. Burwell*, 576 U.S. 473, 486 (2015); *see also Whitman v. Am. Trucking Associations*, 531 U.S. 457, 468 (2001) (explaining that this doctrine is premised on the idea that Congress usually does not “hide elephants in mouseholes”). Here, the Court sees nothing “extraordinary” about this case or the regulatory action taken by OFAC that would implicate the major questions doctrine because, unlike other recent cases in which the doctrine has been applied,<sup>12</sup> the designation of Tornado Cash falls squarely

---

<sup>11</sup> While the phrase “any interest” is a broad one, it is not ambiguous, and “[t]he rule of lenity is not used to narrow a statute that has an unambiguously broad thrust.” *United States v. Litchfield*, 986 F.2d 21, 22 (2d Cir. 1993).

<sup>12</sup> *See, e.g., NFIB v. OSHA*, 142 S.Ct. 661, 662 (2022) (involving a vaccine mandate affecting 80 million workers that was imposed by an occupational safety agency); *Ala. Ass’n of*

within the authority delegated to OFAC and is a targeted action directed at a single entity whose services have been used to launder hundreds of millions of dollars of stolen cryptocurrency for the benefit of the North Korean government.

Accordingly, for the reasons stated above, the Court finds that OFAC did not exceed its statutory authority by designating Tornado Cash.

#### Arbitrary or Capricious

Plaintiffs argue that OFAC's designation of Tornado Cash was arbitrary and capricious because (1) it did not match the OFAC's proffered foreign-affairs rationale, (2) it departed from OFAC's longstanding position of sanctioning persons who can change their behavior rather than technology that cannot, and (3) it failed to consider important aspects of the problem. Defendants responds that OFAC's designation of Tornado Cash was not arbitrary or capricious, that it was reasonable and necessary for national security, and that it satisfies the deferential standard for judicial review under the APA. The Court agrees with Defendants.

An agency's decision is arbitrary and capricious if "the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, [or] offered an explanation for its decision that runs counter to the evidence before the agency." *High Point, LLLP v. Nat'l Park Serv.*,

---

*Realtors v. HHS*, 141 S.Ct. 2485, 2489 (2021) (involving a nationwide eviction moratorium imposed by a public health agency).



850 F.3d 1185, 1193–94 (11th Cir. 2017) (quoting *Miccosukee Tribe of Indians of Florida v. United States*, 566 F.3d 1257, 1264 (11th Cir. 2009)). Here, the Court finds that OFAC’s decision to block Tornado Cash was not arbitrary or capricious for any of the reasons asserted by Plaintiffs.

*First*, there is ample evidence in the administrative record justifying OFAC’s decision to designate Tornado Cash based on the Defendants’ foreign-affairs rationale.<sup>13</sup> Indeed, there is no real dispute that Tornado Cash has been used to help launder hundreds of millions of dollars of stolen cryptocurrency and that some of those funds have benefitted the North Korean government and its nuclear missile program.

*Second*, OFAC’s designation of Tornado Cash does not constitute a departure from the policy of United States’ sanctions policy. Indeed, the designation is consistent with that policy because it is intended “to deter or disrupt behavior that undermines U.S. national security.” Dep’t of the Treasury, *The Treasury 2021 Sanctions Review 1* (2021), <https://perma.cc/9M85-7ZRN>.

*Third*, OFAC did not fail to consider important aspects of the problem, such as reliance interests and loss of property. Indeed, OFAC publicly stated that it would

---

<sup>13</sup> The information in classified lodging provides additional detail about this issue, but it is unnecessary (and would be inappropriate) for the Court to discuss the contents of that information here because, even without that information, there is ample evidence in the administrative record to establish that Tornado Cash has been used to launder the proceeds of illicit activities that has funded the activities of the North Korean government.

not prioritize enforcement against “dusting” transactions, *see* <http://perma.cc/5KQ5-25GE> (FAQ 1078), and OFAC provided a licensing scheme that Plaintiffs (and others) can utilize to complete whatever transactions are necessary to recover assets that are still held in Tornado Cash pools, *id.* (FAQ 1079). These actions demonstrate that OFAC considered the relevant reliance interests and took steps to mitigate any negative consequences innocent Tornado Cash users may face as a result of the designation.

Accordingly, for the reasons stated above, the Court finds that the designation of Tornado Cash was not arbitrary or capricious.

#### First Amendment

Plaintiffs argue that OFAC’s designation of Tornado Cash violated the First Amendment because it chilled Plaintiffs’ protected rights of association by blocking a financial privacy tool they relied on to make donations to organizations and causes and it was not narrowly tailored to achieve its aims. Defendants responds that the First Amendment was not implicated by OFAC’s designation of Tornado Cash and, and even if it was, the designation satisfies the requisite level of scrutiny.

Plaintiffs do not cite any authority supporting the existence of a First Amendment right to use a particular service or type of currency to make donations for charitable or other purposes. The freedom of association cases cited by Plaintiffs are distinguishable because those cases involve government action that compelled



private associations to disclose their major donors or members. *See Americans for Prosperity Found. v. Bonta*, 141 S. Ct. 2373 (2021); *Gibson v. Florida Legislative Investigation Comm.*, 372 U.S. 539 (1963). Here, the designation of Tornado Cash did not compel private associations to disclose anything about their donors or members.

The Court did not overlook Plaintiffs’ reliance on *Meyer v. Grant*, 486 U.S. 414, 424 (1988), for the proposition that the government violates the First Amendment when it “restricts access to the most effective, fundamental, and perhaps economical avenue of political discourse.” However, that case does not help Plaintiffs here for two reasons.

*First*, *Meyer* is a free speech case that dealt with the chilling consequences that a ban on paying the circulators of initiative petitions would have on disseminating “political discourse.” Here, Plaintiffs have raised a freedom of association claim, not a free speech claim.

*Second*, the designation of Tornado Cash does not preclude Plaintiffs (or anyone else) from spending money or donating money for political ends, nor does it preclude organizations from accepting anonymous donations. The fact that Tornado Cash may be Plaintiffs’ preferred way of maintaining their financial privacy does not mean that it is the only way for them to do so. Indeed, it is noteworthy that one of the plaintiffs stated in his declaration that Tornado Cash is used “in his regular

rotation of privacy tools,” Doc. 36-2 at ¶9, which implies that there are other privacy tools that are available to Plaintiffs.

Accordingly, for the reasons stated above, the Court finds that the designation of Tornado Cash did not implicate Plaintiffs’ First Amendment rights.<sup>14</sup>

### **Conclusion**

In sum, for the reasons stated above, it is **ORDERED** that:

1. Plaintiffs’ motion for summary judgment (Doc. 36) is **DENIED**.
2. Defendants’ cross-motion for summary judgment (Doc. 57) is **GRANTED**.
3. The Clerk shall enter judgment stating: “Summary judgment is entered in favor of Defendants. All claims in Plaintiffs’ amended complaint are dismissed with prejudice. Plaintiffs shall take nothing from this action and Defendants shall go hence without delay.”
4. The Clerk shall close the case file.

**DONE and ORDERED** this 30th day of October, 2023.



---

**T. KENT WETHERELL, II**  
**UNITED STATES DISTRICT JUDGE**

---

<sup>14</sup> Based on this conclusion, the Court need not consider what level of scrutiny applies to the designation of Tornado Cash or whether the designation would withstand that level of scrutiny.



**TAB 75**

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF FLORIDA  
PENSACOLA DIVISION**

COIN CENTER et al

VS

CASE NO. 3:22-cv-20375-TKW-ZCB

JANET YELLEN et al

**JUDGMENT**

Pursuant to and at the direction of the Court, it is

ORDERED AND ADJUDGED that Summary Judgment is entered in favor of Defendants. All claims in Plaintiffs' amended complaint are dismissed with prejudice. Plaintiffs shall take nothing from this action and Defendants shall go hence without delay.

JESSICA J. LYUBLANOVITS  
CLERK OF COURT

October 30, 2023  
DATE

/s/ *Monica Broussard*  
Deputy Clerk: Monica Broussard